Office of the New York State Attorney General Letitia James

Economic Justice Division

Stop Addictive Feeds Exploitation (SAFE) for Kids Act

Notice of Proposed Rulemaking

Submitted to the New York State Register
September 15, 2025

Preliminary Statement

The New York State Legislature passed the Stop Addictive Feeds Exploitation (SAFE) for Kids Act (referred to as the "Act" or the "Safe for Kids Act") because New York minors are in the midst of a mental health crisis caused by harmful social media use.[1] The Legislature found that social media companies have created feeds personalized by algorithms. These feeds can track tens or hundreds of thousands of data points about users to create a stream of media that can keep minors scrolling for dangerously long periods of time. Minors, who are less capable than adults of exercising self-control, have been particularly susceptible to these addictive feeds. The Legislature found that these hours spent on social media have caused harm to New York minors including depression, anxiety, suicidal ideation, and self-harm.

The Act prohibits social media platforms from providing minors with an addictive feed, defined as using data concerning a minor (or the minor's device) to personalize the material the minor sees, a feature linked to addictive behavior and extending time spent on social media to unsafe levels. It also prohibits covered platforms from providing nighttime notifications concerning addictive feeds between the hours of 12 AM and 6 AM. The Act allows for parental consent and includes a number of other provisions to ensure all stakeholders can enjoy the benefits of the Act without compromising their experience or their privacy.

The Legislature has charged OAG — which has significant experience with the harms of social media, privacy, and complex technical issues through its investigations and litigations, and through its in-house research and analytics team — with promulgating regulations before the statute can go into effect. The Legislature gave OAG an express directive to promulgate regulations:

- to identify "commercially reasonable and technically feasible methods" to determine that a user is not a minor before providing them with an addictive feed or nighttime notification. (G.B.L. § 1501(1)(a), (2)); and

- to identify methods of obtaining verifiable parental consent for an addictive feed or nighttime notification (G.B.L. § 1501(1)(b), (4)).

In addition, OAG is charged with promulgating regulations to effectuate and enforce the Act as a whole.

The OAG issued an advanced notice of proposed rulemaking on August 1, 2024, providing the public until September 30, 2024, to submit comments. The OAG received 47

[1] 2024 N.Y. Laws ch. 120, section 2.

comments from various interested parties including industry, academia, advocacy organizations, trade organizations, and members of the public. The OAG is grateful for the robust response and carefully reviewed and considered those comments in crafting the proposed rules. The proposed rules reflect not only OAG's research, experience, and expertise but also OAG's reflection on the data, information, and opinions shared by interested parties.

The OAG seeks comment on every aspect of the proposed rules including personal experiences, research, technology standards, and industry information, together with examples, data, and analysis in support of any comment. The OAG seeks the broadest participation and urges interested parties to submit written comments and to share this proposal widely. This includes all New Yorkers, New York parents and other caretakers of minors, New York minors, New York educators, members of academia, consumer advocacy groups, privacy advocacy groups, industry participants, and other members of the public.

Table of Contents

I. Rule Text

Part 700—SAFE for Kids Act

Proposed Action: Add Part 700 of Title 13 NYCRR

Statutory Authority: General Business Law, Article 45, 1500-1508

Subject: SAFE for Kids Act

Purpose: Implement the SAFE for Kids Act as directed by Article 45 of General Business Law, specifically and as necessary to effectuate and enforce Article 45.

Text of proposed rule:

700.1 Definitions

For purposes of this Part:

(a) *Accredited Third-Party.* The term *Accredited Third-Party* means a person recognized by the American National Standards Institute (ANSI) or equivalent accreditation body, in accordance with the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 17065:2012: Conformity assessment — Requirements for bodies certifying products, processes and services or an equivalent industry standard, as qualified to certify an age assurance method.

(b) *Accuracy Minimum.* The term *Accuracy Minimum* means:

(1) a rate of false positives for an age assurance method that is equal to or less than the following: 0.1% of minors ages 0 to 7; 1% of minors ages 8 to 13; 2% of minors ages 14 to 15; 8% of minors age 16; 15% of minors age 17, excluding failures or refusals by a user to provide requested data and inconclusive age assurance outcomes; and

(2) a rate of detecting method circumvention for an age assurance method that meets or exceeds 98%.

(c) Addictive Feed. The term *Addictive Feed* means an online platform, or a portion thereof, in which multiple pieces of media from an online platform are:

(1) shared or generated by users, and

(2) concurrently or sequentially, recommended, selected, or prioritized for display to a user based, in whole or in part, on

(i) information persistently associated with the user or the user's device; or

(ii) the user's previous interactions with media generated or shared by other users including the user's interactions on different online platforms, media or the pages, groups, or other user-generated media the user requests, subscribes to, otherwise selects, or a combination thereof.

(3) The following conduct does not constitute an addictive feed:

(i) the recommendation, prioritization, or selection of media based on user-selected privacy or accessibility settings, or technical information concerning the user's device;

(ii) the display of specific media in response to express and unambiguous user requests or media by an author, creator, or poster of media the user subscribes to;

(iii) the display of media users share to a page or group the user subscribes to;

(iv) the display of media where the user expressly and unambiguously requests

(*a*) the specific media;

(*b*) the media of a specified author, creator, or poster of media;

(*c*) the media users to a page or group share; or

(*d*) that specific media or the media of a specified author, creator, or poster of media be blocked, prioritized or deprioritized for display;

(v) the display of media that is a direct and private communication;

(vi) the recommendation, prioritization, or selection of media only in response to a specific search inquiry by the user;

(vii) the recommendation, prioritization, or selection of media for display where the media is exclusively next in a pre-existing sequence from the same author, creator, poster, or source; or

(viii) the recommendation, prioritization, or selection of media that is necessary to comply with the provisions of this Part and any regulations promulgated pursuant to this Part.

(d) *Addictive Online Platform.* The term *Addictive Online Platform* means an online platform that offers or provides users one or more addictive feeds as a significant part of the services provided by such online platform. An addictive feed or multiple addictive feeds jointly are a significant part of the services provided by an online platform if 20 percent or more of time

spent by monthly active users on an online platform is spent on addictive feeds measured over any six-month period in the prior calendar year.

(e) *Adult.* The term *Adult* means an individual 18 years of age or older.

(f) *Affiliate.* The term *Affiliate* is any person that directly, or indirectly through one or more intermediaries, controls, is controlled by, or is under common control with the person specified.

(g) *Age Status.* The term *Age Status* means the state of being a minor or an adult.

(h) *Age Assurance Method.* The term *Age Assurance Method* means any type of age estimation, age inference, or age verification.

(i) *Age Estimation.* The term *Age Estimation* means to use analysis of a physical or behavioral feature to draw a conclusion regarding an individual's age or age status.

(j) *Age Inference.* The term *Age Inference* means to use verified information other than age to draw a conclusion regarding an individual's age or age status.

(k) *Age Verification.* The term *Age Verification* means to use generally accepted identification, including government-provided identification, or validation against an official records source, to confirm an individual's age or age status.

(l) *Certification.* The term *Certification* means the confirmation by an accredited third-party that an age assurance method meets (i) ISO/IEC 27566:2025 Information security, cybersecurity and privacy protection — Age assurance systems, Institute for Electrical and Electronics Engineers 2089.1-2024 Standard for Online Age Verification, or an equivalent industry standard; (ii) the accuracy minimum; and (iii) the testing requirements in section 700.5(b) of this Part. "Certify" means the act of certification and "certified" means having received certification.

(m) *Covered Minor.* The term *Covered Minor* means a user of an online platform in the State of New York for whom the covered operator has actual knowledge the user is a minor.

(n) *Covered Operator.* The term *Covered Operator* means any person who operates or provides an addictive online platform and the person's agents and affiliates involved in operating or providing an addictive online platform or complying with this Part.

(o) *Covered User.* The term *Covered User* means a user of an online platform in the State of New York, not acting as an operator, or agent or affiliate of the operator of such online platform or any portion thereof.

(p) *Delete.* The term *Delete* means to permanently destroy, remove, or de-identify information using reasonable measures to protect against the unauthorized access or use of such information and to ensure that such information may not be retrieved after the deletion process has been completed. For purposes of this section, to de-identify information, a covered operator must:

(1) take reasonable measures to de-identify any information that identifies or can reasonably be linked to an individual or device;

(2) take reasonable measures to ensure the de-identified information cannot be re-linked with an individual or device;

(3) not process and must publicly commit not to process the de-identified information except only in its de-identified state, and must not attempt and must publicly commit not to attempt to re-identify or re-link the de-identified information;

(4) take reasonable measures to ensure any recipients of de-identified information also abide by these restrictions; and

(5) take reasonable measures to ensure that the de-identified information is only retained as long as necessary to fulfill the purposes permitted under this Part and is not used for any other purpose.

(q) *Exempt Online Platform.* The term *Exempt Online Platform* means an online platform that meets the definition of addictive online platform and has fewer than 5 million monthly active users or fewer than 20,000 monthly active users who are covered minors, except addictive online platforms whose primary user base is minors are not exempt online platforms.

(r) *False Negative.* The term *False Negative* means incorrectly identifying an adult as a minor.

(s) *False Positive.* The term *False Positive* means incorrectly identifying a minor as an adult.

(t) *Inconclusive Age Assurance Outcome.* The term *Inconclusive Age Assurance Outcome* means following receipt of all requested information from a user, and absent detection of method circumvention, a determination that the age assurance method cannot provide an age or age status for that user.

(u) *Information Persistently Associated.* The term *Information Persistently Associated* means any information that a covered operator associates with a user or a user's device over time. Information is not persistently associated if the covered operator does not use the information to recognize the user or the user's device over time.

(v) *Media.* The term *Media* means text, an image, or a video.

(w) *Method Circumvention.* The term *Method Circumvention* means submission of false data or interference with an age assurance method.

(x) *Minor.* The term *Minor* means an individual under 18 years of age.

(y) *Monthly Active User.* The term *Monthly Active User* means an individual who, in the previous calendar month or the one-month average measured across the previous quarter, accesses an online platform and remains on the online platform for at least one minute.

(z) *Nighttime Notifications.* The term *Nighttime Notifications* means notifications concerning an addictive feed between the hours of 12 AM Eastern and 6 AM Eastern. Notifications required by applicable federal, state, or local laws are not nighttime notifications.

(aa) *Online Platform.* The term *Online Platform* means a website, online service, online application, or mobile application.

(bb) *Operator.* The term *Operato*r means any person that operates or provides an online platform

(cc) *Parent.* The term *Parent* means an individual who is recognized under State law as:

(1) acting in parental relation to the covered minor;

(2) having the status of a legal guardian or custodian for the covered minor; or

(3) in the case of an individual who otherwise would qualify as a minor, having the status of a parent to the covered minor.

(dd) *Person.* The term *Person* means an individual, partnership, corporation, association, or any other form of business enterprise.

(ee) *Self-Declaration.* The term *Self-Declaration* means an action by a covered user, such as a representation in writing or clicking on a confirmation button, indicating the covered user's age or age status.

(ff) *Technical Information Concerning a User's Device.* The term *Technical Information Concerning a User's Device* means information that is associated with the user's device and technical in nature. Technical information concerning a user's device:

(1) is not information linked to the user's identity;

(2) cannot include information linked, directly or indirectly, to the user's previous interactions with media generated or shared by other users; and

(3) is not otherwise processed for the purpose of providing an addictive feed or nighttime notifications.

(gg) *Total Accuracy Minimum.* The term *Total Accuracy Minimum* means:

(1) a combined rate of false positives and inconclusive age assurance outcomes for an age assurance method that is equal to or less than the following: 0.1% of minors ages 0 to 7; 1% of minors ages 8 to 13; 2% of minors ages 14 to 15; 8% of minors age 16; 15% of minors age 17, excluding failures or refusals by a user to provide requested data; and

(2) a rate of detecting method circumvention that meets or exceeds 98%.

(hh) *User.* The term *User* means a person that uses a covered operator's online platform or any portion thereof and is not acting as the covered operator or an agent or affiliate of the covered operator.

(ii) *Valid Consent.* The term *Valid Consent* means consent that is clear and unambiguous, specific, informed, and freely granted.

(1) "Clear and unambiguous" means an expression of consent through an individual's affirmative action.

(2) "Specific" means the request for consent is presented separately from any other request by the covered operator. A covered operator may request consent for an addictive feed and for nighttime notifications in a single transaction, provided that an individual may grant or refuse consent separately for each feature.

(3) For purposes of sections 700.2 and 700.3 of this Part, "informed" means a notice pursuant those sections that is provided in plain language and is understandable and accessible to the target audience. Any such notice must be provided in at least the twelve most commonly spoken languages in the State of New York consistent with section 202-a of the Executive Law, and may be provided in written or any other form that otherwise complies with these regulations.

(4) “Freely granted” means that the mechanism for refusing consent is at least as easy to use as the mechanism for granting consent and any previously granted consent may be easily modified or withdrawn at any time.

(jj) *Zero-Knowledge Proof Age Assurance.* The term *Zero-Knowledge Proof Age Assurance* means a cryptographic technique that allows an individual to demonstrate age status using verified data without revealing additional information to the operator or any third-party beyond the validity of the individual’s age status.

700.2 Prohibition of Addictive Feeds

(a) It shall be unlawful for a covered operator to provide an addictive feed to a covered user unless:

(1) the covered operator completes an age assurance method consistent with section 700.4 of this Part to determine the covered user is not a covered minor and the covered operator does not otherwise have actual knowledge of the covered user’s minor age status; or

(2) the covered user is a covered minor and the covered operator has obtained verifiable parental consent consistent with subdivision (e) of this section to provide an addictive feed to the covered minor.

(b) A covered operator is not required to provide a covered minor access to a method of verifiable parental consent for addictive feeds.

(c) Exempt online platforms are exempt from the requirements of this Part. If an addictive online platform no longer qualifies as an exempt online platform, it has 180 days from the first such instance and 30 days from any subsequent instances before it must comply with subdivision (a) of this section.

(d) In determining whether a user is a covered user, a covered operator must

(1) take into account all reliable information accessible by the covered operator regarding the user’s location including technical information concerning a user’s device and covered user data the covered operator possesses or accesses for marketing, content selection, or other commercial purposes; and

(2) take reasonable steps to investigate and detect covered user efforts to conceal or misrepresent their location and, in such instances, employ reasonable methods utilizing available data to determine whether the user is a covered user.

(e) Verifiable parental consent requirements for addictive feeds.

(1) Consent requirements

(i) Consent from a covered minor. To request verifiable parental consent under paragraph (2) of subdivision (a) of this section, a covered operator must:

(*a*) provide the covered minor notice that the covered operator cannot legally provide the covered minor an addictive feed without verifiable parental consent; and

(*b*) obtain valid consent from the covered minor to request verifiable parental consent for an addictive feed.

(ii) Consent from the parent. If a covered minor provides valid consent consistent with subparagraph (i) of paragraph (1) of subdivision (d) of this section, a covered operator must:

(*a*) provide the parent with notice that the covered operator cannot legally provide the covered minor an addictive feed without verifiable parental consent; and

(*b*) offer the parent access to a method of verifiable parental consent that meets the requirements of this section.

(2) Withdrawal of consent. A covered operator must provide covered minors and parents a simple, accessible mechanism to withdraw consent for an addictive feed at any time. The mechanism to withdraw consent must be at least as easy to use as the mechanism used to give consent. In no event shall a covered minor or parent be required to interact with a live representative to withdraw consent if they did not do so to give consent.

(3) Renewed request for consent. If a parent refuses valid consent for an addictive feed, a covered operator may renew a request for consent from a parent only at the request of the covered minor.

(4) Notice requirements. The notice required by subdivision 2(e)(1)(i) and (ii) of this section must be clear and conspicuous, and provided at or before any request for consent. The notice must:

(i) identify the addictive online platform;

(ii) identify the covered minor's account, or profile, or username, as applicable;

(iii) provide the following information with equal prominence and in plain language that is understandable and accessible to the target audience:

(*a*) the law of the State of New York does not allow the covered operator to provide media to a minor using a feature in which the operator recommends, selects, or prioritizes media based on information associated with that minor without parental consent except in limited circumstances.

(*b*) the minor can access the platform with a feed that does not include this feature including while any request for consent under this section is pending; and

(*c*) a covered minor or parent can modify or withdraw their consent.

(5) Methods of verifiable parental consent. Any verifiable parental consent method must:

(i) determine the parent's age status pursuant to section 700.4 of this Part, providing any instructions to the parent in at least the 12 most commonly spoken languages in the State of New York consistent with section 202-a of the Executive Law, in written or any other form that otherwise complies with these regulations;

(ii) give the parent the option to provide valid consent;

(iii) be reasonably calculated, in light of available technology, to ensure that the individual providing consent is a parent of the covered minor;

(iv) make reasonable efforts to protect the covered users' and parents' privacy and safety;

(v) be reasonably calculated, in light of available technology, to account for the likelihood of circumvention, fraud, or misuse of the method;

(vi) include at least one option that does not require the parent to furnish government-provided identification unless the covered operator collects or possesses a parent's government-provided identification to comply with other laws and obtains consent to use the same for verifiable parental consent; and

(vii) include at least one option that does not require the parent to create an account with the covered operator or require the parent to purchase additional goods or services from the covered operator.

(6) Notwithstanding the requirements of this subdivision (e), if an addictive online platform is a "website or online service directed to children," under 15 U.S.C. § 6501(10) and its implementing regulation 16 C.F.R. § 312.2, or if a user is a covered minor under 13, a covered operator may use the methods for verifiable parental consent listed under 16 C.F.R. § 312.5, provided:

(i) the covered operator provides the parent with notice as required by paragraph (4) of this subdivision (e);

(i) the covered operator complies with paragraph (5) of this subdivision; and

(iii) the method is reasonably calculated, in light of available technology, to account for the reasonable likelihood of circumvention, fraud, or misuse of the method.

(7) A covered operator must review and update any verifiable parental consent method at least annually to ensure continued compliance with this section.

700.3 Prohibition of Nighttime Notifications

(a) It shall be unlawful for a covered operator to provide nighttime notifications to a covered user unless:

(1) the covered operator uses an age assurance method consistent with section 700.4 of this Part to determine the covered user is not a covered minor and the covered operator does not otherwise have actual knowledge of the covered user's minor age status; or

(2) the covered user is a covered minor and the covered operator has obtained verifiable parental consent consistent with subdivision (e) of this section to provide nighttime notifications to the covered minor.

(b) A covered operator is not required to provide a covered minor access to a method of verifiable parental consent for nighttime notifications.

(c) Exempt online platforms are exempt from the requirements of this Part. If an addictive online platform ceases to be an exempt online platform, it has 180 days from the first such instance and 30 days from any subsequent instances before it must comply with subdivision (a) of this section.

(d) In determining whether a user is a covered user, a covered operator must

(1) take into account all reliable information accessible by the covered operator regarding the user's location including technical information concerning a user's device and covered user data the covered operator possesses or accesses for marketing, content selection, or other commercial purposes; and

(2) take reasonable steps to investigate and detect covered user efforts to conceal or misrepresent their location and, in such instances, employ reasonable methods utilizing available data to determine whether the user is a covered user.

(e) Verifiable parental consent for nighttime notifications.

(1) Consent requirements.

(i) Consent from a covered minor. To request verifiable parental consent under paragraph (2) of subdivision (a) of this section, a covered operator must:

(*a*) provide the covered minor notice that the covered operator cannot legally provide the covered minor nighttime notifications without verifiable parental consent; and

(*b*) obtain valid consent from the covered minor to request verifiable parental consent for nighttime notifications.

(ii) Consent from the parent. If a covered minor provides valid consent consistent with subparagraph(i) of this paragraph, a covered operator must:

(*a*) provide the parent with notice that the covered operator cannot legally provide the covered minor nighttime notifications without verifiable parental consent; and

(*b*) offer the parent access to a method of verifiable parental consent that meets the requirements of this section.

(2) Withdrawal of consent. A covered operator must provide covered minors and parents a simple, accessible mechanism to withdraw consent for nighttime notifications at any time. The mechanism to withdraw consent must be at least as easy to use as the mechanism used to give consent. In no event shall a covered minor or parent be required to interact with a live representative to withdraw consent if they did not do so to give consent.

(3) Renewed request for consent. If a parent refuses valid consent for nighttime notifications, a covered operator may renew a request for consent from a parent only at the request of the covered minor.

(4) Notice requirements. The notice required by subparagraphs (1)(i) and (ii) of this subdivision must be clear and conspicuous, and provided at or before any request for consent. The notice must:

(i) identify the addictive online platform;

(ii) identify the covered minor's account, or profile, or username, as applicable;

(iii) provide the following information with equal prominence and in plain language that is understandable and accessible to the target audience:

(*a*) the law of the State of New York does not allow the covered operator to provide notifications between the hours of 12 AM Eastern and 6 AM Eastern to a covered minor concerning a feed that uses a feature in which the operator recommends, selects, or prioritizes media based on information associated with that minor without parental consent except in limited circumstances;

(*b*) the minor can access the platform without these nighttime notifications including while any request for consent under this section is pending; and

(*c*) a covered minor or parent can modify or withdraw their consent.

(5) Methods of verifiable parental consent. Any verifiable parental consent method must:

(i) determine the parent's age status pursuant to section 700.4 of this Part, providing any instructions to the parent in at least the twelve most commonly spoken languages in the State of New York consistent with section 202-a of the Executive Law, in written or any other form that otherwise complies with these regulations;

(ii) give the parent the option to provide valid consent;

(iii) be reasonably calculated, in light of available technology, to ensure that the individual providing consent is a parent of the covered minor;

(iv) make reasonable efforts to protect the covered users' and parents' privacy and safety;

(v) be reasonably calculated, in light of available technology, to account for the likelihood of circumvention, fraud, or misuse of the method;

(vi) include at least one option that does not require the parent to furnish government-provided identification unless the covered operator collects or possesses a parent's government-provided identification to comply with other laws and obtains consent to use the same for verifiable parental consent; and

(vii) include at least one option that does not require the parent to create an account with the covered operator or require the parent to purchase additional goods or services from the covered operator.

(6) Notwithstanding this subdivision, if an addictive online platform is a "website or online service directed to children," under 15 U.S.C. § 6501(10) and its implementing regulation 16 C.F.R. § 312.2, or if a user is a covered minor under 13, a covered operator

may use the methods for verifiable parental consent listed under 16 C.F.R. § 312.5, provided

(i) the covered operator provides the parent with notice as required by section paragraph (2) of this subdivision;

(ii) the covered operator complies with paragraph (5) of this subdivision; and

(iii) the method is reasonably calculated, in light of available technology, to account for the reasonable likelihood of circumvention, fraud, or misuse of the method.

(7) A covered operator must review and update any verifiable parental consent method at least annually to ensure continued compliance with this section.

700.4 Actual Knowledge of Minor Age Status and Age Assurance Methods

(a) The following individually or jointly constitute actual knowledge of a covered user's minor age status for purposes of this Part:

(1) Self-declaration of minor age status, provided that such self-declaration is requested by the covered operator or otherwise can reasonably be associated with the covered user;

(2) A covered operator's use of one or more age assurance methods consistent with paragraph (1) of subdivision (b) of this section that results in a determination of minor age status;

(3) A covered operator's possession or access to covered user data for marketing, content selection, or other commercial purposes that, if applied to an age assurance method the covered operator provides, would result in a determination of minor age status; or

(4) The covered operator's good faith determination based on other, reliable evidence or knowledge that the covered user is a minor.

(b) To determine that a covered user is not a covered minor, covered operators must:

(1) Provide covered users one or more age assurance methods, each of which must be certified consistent with section 700.5 of this Part to meet the accuracy minimum and at least one of which must be certified consistent with section 700.5 of this Part to meet the total accuracy minimum; and either

(i) Receive a determination that the covered user has adult age status from at least one age assurance method provided to users pursuant to paragraph (1) of subdivision (b) of this section; or

(ii) If all of the following are present, presume a covered user has adult age status:

(*a*) age assurance methods offered by the covered operator pursuant to paragraph (1) of subdivision (b) of this section are completed for the covered user, including at least one age assurance method that meets the total accuracy minimum,

(*b*) each of the methods is inconclusive, and

(*c*) the covered operator otherwise has no actual knowledge that the covered user is a covered minor.

(c) If the covered operator provides age verification using government-provided identification as an age assurance method, the covered operator must:

(1) accept government-provided identification from all U.S. and non-U.S. jurisdictions;

(2) allow a user to proceed to the appeals process described in section 700.6 of this Part if all other age assurance methods offered by the covered operator are inconclusive and the user declines to provide government-provided identification; and

(3) provide at least one age assurance method that does not require the furnishing of government-provided identification unless the covered operator necessarily collects or possesses such identification to comply with other laws or offers the user a zero-knowledge proof age assurance method.

(d) With respect to investigations or changes in age status of covered users, a covered operator must:

(1) change a covered user's adult age status to minor within 10 business days if the covered operator obtains actual knowledge that the covered user is a minor;

(2) conduct an investigation of any report or information indicating a covered user has minor age status or has falsified data related to adult age status, including through method circumvention, sufficient to determine whether the report or information constitutes reliable evidence of minor age status;

(3) conduct an investigation of new or previously undetected forms of method circumvention, including in response to public reports, direct reports to the operator or its agents, and monitoring of changes in aggregate age assurance outcomes consistent

with undetected method circumvention, and if validated, take sufficient steps to correct resulting false positives and effectively detect the form of method circumvention in the future; and

(4) provide covered minors a process to update their minor age status upon reaching adult status, at which time the covered user must undergo an age assurance method pursuant to subdivision (b) of this section.

(e) A covered operator must make available to covered users an explanation of any age assurance methods offered and, in the event covered user data is requested, the purpose of the data request, how the data will be used, and when and how the data will be deleted.

(f) Covered operators may not introduce any design feature that discourages covered users from participating in or successfully completing an age assurance method or facilitates method circumvention by covered users.

(g) Covered operators must, initially and periodically thereafter, evaluate the accuracy, method circumvention, and user burden of their age assurance methods against alternative commercially reasonable age assurance methods that otherwise comply with the obligations in this Part. Covered operators must act reasonably and in good faith to adopt more effective age assurance methods consistent with related industry and technological developments, including commercially reasonable age assurance methods with lower false positive and false negative outcomes and maximum method circumvention detection rates.

700.5 Certification of Age Assurance Methods

(a) A covered operator must obtain a certification annually for each age assurance method it offers.

(b) Certification of an age assurance method must include the following testing, which must be documented in a written report including testing protocols used and all results:

(1) false positive rate for ages 0-17; the data must be reported in aggregate and disaggregated by the age categories in the accuracy minimum;

(2) rate of inconclusive age assurance outcomes and the reason for each inconclusive age assurance outcome;

(3) false negative rate for ages 18-30; the data must be reported in aggregate and disaggregated by age categories 18, 19-20, 21-25, and 26-30;

(4) detection of method circumvention through testing consistent with a nationally or internationally recognized standard, or if none is available, including a variety of attack

vectors weighted to reflect the most prevalent risks, with documentation of the quantity and type of attack methodologies tested;

(5) data collection, segregation, and deletion measures, in accordance with section 700.7 of this Part;

(6) data encryption and security measures; and

(7) determination of whether the age assurance method meets the accuracy minimum and total accuracy minimum.

(c) Test data used for certification of the accuracy minimum and the total accuracy minimum, and to fulfill the testing requirements in subdivision (b) of this section, must meet the following requirements:

(1) Sample size calculation must yield reliable and statistically significant results with a high confidence level and low margin of error using as a baseline the population of the State of New York most recently reported by the U.S. Census Bureau.

(2) Any images in a test dataset must reflect variation in photographic conditions, subject presentation, pose variation, and facial archetypes.

(3) The age assurance method being tested must not have been trained or tuned on the testing dataset or any substantially overlapping dataset.

(d) Covered operators must maintain copies of all test results, reports, and certifications generated in compliance with this section for no less than 10 years.

(e) To the extent an age assurance method has variable settings or options, a covered operator must only use settings or options for which the age assurance method received certification.

(f) In the event at least one ANSI-recognized or equivalent industry certification consistent with the requirements of this Part is not available for an age assurance method, covered operators may work with an accredited third-party to configure testing protocols consistent with subdivision (c) of this section and must retain records of the protocols and testing results.

700.6 Appeals Process

(a) A covered operator shall implement a process for a user to appeal a covered operator's classification of that user as a covered minor. The covered operator must:

(1) offer one or more methods for a user to submit information and documentation in support of the user's adult age status, including at least one option for documentation other than government-provided identification;

(2) evaluate the information and documentation submitted by the user;

(3) make a good faith determination as to whether the information and documentation provide a reasonable basis to reverse the covered operator's previous conclusion regarding the covered user's age status; and

(4) provide a written summary to the user of its decision, including an explanation of the basis for the decision.

(b) The process required by subdivision (a) of this section must be clear, conspicuous, and accessible.

(c) The covered operator must communicate the determination of the user's appeal or request additional information from the user within 10 business days of receipt of the appeal. Where the covered operator requests additional information, the final determination of the appeal must be made and sent to the user expeditiously following receipt of the requested information.

(d) Notwithstanding the requirements in section 700.2 and section 700.4 of this Part, a covered operator may change a covered user's age status from minor to adult based upon the covered operator's determination of age status through the process required by this section.

700.7 Data Use and Protection

(a) Data collected for the purpose of complying with this Part:

(1) shall be the minimum necessary to comply with this Part;

(2) shall not be used for any purpose other than to comply with this Part;

(3) shall be collected and stored using industry-standard data security measures and as required by law, including encryption in transit and at rest; and

(4) shall be held for the minimum time required to comply with this Part and thereafter must be immediately deleted except as provided by subdivision (b) of this section.

(b) Covered operators must retain the following where applicable, for no less than 10 years:

(1) the fact that an age assurance method was attempted on a user;

(2) the age assurance method that successfully confirmed age status;

(3) the date on which an age assurance method resulting in determination of age status was conducted;

(4) the age status of the covered user;

(5) information collected to comply with this Part where necessary for compliance with any applicable provisions of State law or federal law or regulation; and

(6) for each age assurance method utilized, on a month-by-month basis:

(7) the total number of covered users who attempted to confirm age status using that method;

(8) the total number of covered users for whom the covered operator successfully determined age status using that method;

(9) the total number of covered users for whom the covered operator had successfully determined an adult age status using that method who the covered operator subsequently determined were covered minors; and

(10) the total number of covered users denied adult status due to method circumvention.

(c) Covered operators may retain the estimated age of a covered user solely to determine age status for purposes of this Part with the covered user's valid consent.

(d) Nothing in this section shall be construed to regulate data that is collected for a purpose that is unrelated to compliance with this Part.

(e) A covered operator must comply with all other applicable data protection and security laws. In case of conflict, the law that is more protective of a covered minor's privacy and safety shall govern.

(f) Except as set forth in subdivision (b) of this section, nothing in this section shall be construed to require retention of data that identifies an individual user or to allow a covered operator to use data retained pursuant to this section, whether alone or together with other data, in order to identify an individual user.

700.8 Remedies

The Attorney General may bring an action or special proceeding on behalf of the State of New York consistent with section 1508 of the General Business Law whenever it appears

that any person has engaged in or is about to engage in any of the acts or practices in the State of New York stated to be unlawful in Article 45 of the General Business Law and the implementing regulations in this Part.

700.9 Miscellaneous

(a) All requirements herein apply equally to covered operators that elect to engage or otherwise rely upon any third-party to comply with this Part.

(b) Other than as necessary to comply with section 700.2 and section 700.3 of this Part, a covered operator must not:

(1) withhold any product, service, or feature from a covered minor or a parent;

(2) degrade or lower the quality of any product, service, or feature used by a covered minor or a parent; or

(3) increase the price of any product, service, or feature used by a covered minor or a parent.

(c) Except as expressly specified, nothing in this Part shall be construed as requiring a covered operator to give a parent any additional access to or special control over the data or accounts of a covered minor using an addictive online platform.

(d) Except as expressly and specifically required in in this Part or as strictly necessary to comply with applicable laws, any notice provided by a covered operator in order to comply with this Part shall not disclose any information to the parent that reveals a covered user's use of, or other activity associated with the addictive online platform. Specifically, but not exclusively, a covered operator's notice shall not disclose:

(1) personalized attributes associated with the covered minor;

(2) content selections or interactions associated with the covered minor;

(3) specific pieces of content that may be accessible via the addictive feed, or that may be included in nighttime notifications;

(4) identities of other users of the addictive online platform; and

(5) settings choices made by the covered minor.

700.10 Severability

The provisions of this Part shall be severable, and if any item, subclause, clause, sentence, subparagraph, paragraph, subdivision, section, or subpart of this Part, or the applicability thereof to any person or circumstances, shall be adjudged by any court of competent jurisdiction to be invalid, such judgment shall not affect, impair or invalidate the remainder thereof, nor the application thereof, but shall be confined in its operation to the item, subclause, clause, sentence, subparagraph, paragraph, subdivision, section, or subpart thereof, or to the person or circumstance directly involved in the controversy in which such judgment shall have been rendered.

700.11 Effective Date

This Part shall take effect on the 180th day after publication in the State Register.

II. Regulatory Impact Statement

A. Statutory Authority

General Business Law ("G.B.L.") sections 1501(2), 1501(4), 1505, and 1506(2) authorize the Attorney General ("OAG") to promulgate rules to effectuate and enforce Article 45 of the G.B.L., the Stop Addictive Feeds Exploitation (SAFE) for Kids Act ("the Act" or "SAFE for Kids Act").[1]

B. Legislative Objectives

The primary objective of the Act is to address the dramatic negative effect of addictive feeds on minors by prohibiting social media companies from providing individuals under 18 years of age with addictive feeds absent parental consent.[2] The Legislature carefully weighed the interests of all stakeholders—including minors, parents and caregivers, and social media companies—in adopting the Act.

The proposed rule implements the Legislature's goals of ensuring covered platform operators have a framework for commercially reasonable and technically feasible methods they can use to determine user age. The proposed rule also facilitates covered platforms' ability to implement methods for verifiable parental consent and provides operators guidance and clarity where possible with respect to coverage and the requirements of the Act.

1. What are addictive online platforms?

The rise of social media use by minors is well-documented as are the staggering negative trends in the mental health of minors. Understanding the relationship between the two requires looking back at the history of how social media evolved. Early iterations of social media allowed users to connect with each other and displayed content created by a user's connections, usually chronologically, to provide the latest updates from friends and family. Over time, users' networks grew, and platforms introduced advertising in the form of "sponsored" content that appeared alongside the organic content posted by individual users, increasing the volume of content available for consumption.

---

[1] L. 2024, ch. 120.

[2] L. 2024, ch. 120 § 1.

Social media platforms then began to introduce algorithms using machine learning capabilities to analyze posted content as well as user data and behavior.[3] Some algorithms were created to respond to search queries or to flag inappropriate content. However, platforms primarily evolved their use of algorithms to maximize individual user engagement, including how many hours a day and times a day someone uses the platform. The term "engagement algorithm" is used to describe the feature that encourages a user to continue to use and return to a platform.[4]

Today, social media companies have sophisticated engagement algorithms that produce individually personalized addictive feeds and use notifications as core engagement features. The algorithms vary by platform but consistently leverage user data to keep users engaged.[5] This practice is now inherent to the platforms' business model, referred to as the "attention economy,"[6] because the maximization of user engagement is directly correlated with the platforms' revenue: the more often users visit a platform and the more time they spend per visit, the more money that platform makes. Social media platforms thus are financially incentivized to keep users "scrolling" as long and as often as possible, even at the cost of the users' mental health and well-being.

To maximize revenue from user time and attention, the platforms' engagement algorithms ingest thousands of data points related to each specific user and then organize and deliver an essentially endless "feed" of media that is personalized to that user.[7] Under the original model of social media, the user's engagement or interest might reach a natural end, for example, when they finished viewing the latest media posted by their networks. Now, often there is never an end— the algorithms continually offer up new and eye-catching media based

---

[3] Balaji, Annavarapu, Bablani, *Machine learning algorithms for social media analysis: a survey*, Computer Science Review, Vol. 40, May 2021.

[4] Arvind Narayanan, *Understanding Social Media Recommendation Algorithms* 18, Knight First Amend. Inst. at Columbia Univ. (2023), https://knightcolumbia.org/content/understanding-social-media-recommendation-algorithms.

[5] *Id.* 18-22.

[6] Frank Rose, *The Attention Economy 3.0*, 44-47, Miliken Institute Review, July 2015, https://www.milkenreview.org/articles/the-attention-economy-3-0.

[7] An online platform may simultaneously run multiple algorithms, each performing a different, independent function, as part of the overall feed delivery process. Engagement algorithms are merely one type of algorithm, so turning off an engagement algorithm does not stop the platform from delivering, sharing, prioritizing, or restricting general content. Engagement algorithms also are different from content moderation algorithms that flag or remove content in accordance with, for example, a platform's trust and safety guidelines.

on signals in the user's behavior. Similarly, algorithms determine which content might bring a disengaged user back to the platform and generate notifications delivered directly to the user to facilitate that re-engagement.

User data is gathered with and without the user's awareness. It encompasses information inherent to the user such as location, age, and gender, content the user has previously engaged with, the behavior of other individuals in the user's network or with a similar profile, and how the user reacts to content suggested by the algorithm. The data can also include user behavior on other platforms, gathered via cookies and tracking pixels.[8] The sophistication of the algorithms and the ever-increasing amount of user data fed to them gives the platforms a powerful ability to personalize content that maximizes user attention.[9] Even passive signals undetectable by a human, such as the number of seconds a user lingers on a post, can feed the algorithms that then select and deliver more and more content and notifications.

Algorithmic personalization has made social media platforms a substantial consumer of users' time and mental capacity. While even adult users struggle to moderate their consumption of social media, minors have become significant users of the same platforms and are suffering damaging mental health effects.

2. Mental health harms of addictive feeds and notifications

As described in Part II.B.1, minors' use of social media today is propelled by sophisticated engagement algorithms that leverage minors' data to keep them on and returning to social media platforms. The engagement features targeted by the Act present a well-documented and profound risk to minors' mental health and overall well-being, leading parents, educators, and mental health professionals to call for measures to protect minors.[10]

These features induce "problematic use" of social media in minors, defined as a pattern of compulsive use suggesting a person cannot control their emotional state or their behavior

---

[8] *See* Federal Trade Commission, *A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services*, Sept. 2024, at i.

[9] Youyou, Kosinski, Stilwell, *Computer-based personality judgments are more accurate than those made by humans*, PNAS, Jan. 12, 2015, https://www.pnas.org/doi/full/10.1073/pnas.1418680112.

[10] *See, e.g.*, U.S. Surgeon Gen., Advisory, *Social Media and Youth Mental Health* 9 (2023); *Protecting Our Children Online: Hearing Before the S. Comm. On the Judiciary*, 118th Cong. 109–11 (2023) (statement of Mitch Prinstein, Chief Sci. Officer, Am. Psych. Ass'n); Office of the Minn. Att'y Gen., *Minnesota Attorney General's Report on Emerging Technology and Its Effects on Youth Well-Being* 14 (2025); Anne J. Maheux et al., *Annual Research Review, Adolescent Social Media Use Is Not a Monolith: Toward the Study of Specific Social Media Components and Individual Differences*, J. Child Psych. & Psychiatry 440 (2025).

regarding a given activity.[11] Commonly-accepted signs of problematic social media use include: 1) using social media even when the individual wants to stop, or realizing such use interferes with necessary tasks; 2) spending excessive efforts to ensure uninterrupted access to social media; 3) feeling strong cravings to use social media; 4) disrupting other activities when the individual cannot use social media and cannot control their longing to use social media; 5) consistently spending more time on social media than planned; 6) lying or other deceptive behavior to retain access to social media; and 7) losing or disrupting significant relationships or educational opportunities because of social media use.[12] Problematic use is commonly referred to as addiction and also called addictive use.[13]

Increasingly, problematic use of social media is reported by and observed in minors.[14] For example, in one recent study, 61% of minors report that they failed when they tried to stop or reduce their social media use.[15] Parents similarly describe striking behavioral changes in their minors around uncontrolled use of social media, as well as difficulty in finding coping strategies.[16] These problematic use behaviors are linked to minors' self-control mechanisms,

---

[11] Nat'l Acads. Sci., Eng'g, & Med., *Social Media and Adolescent Health* 109-11 (2024).

[12] Am. Psych. Ass'n, *Health Advisory on Social Media Use in Adolescence* 7 (2023).

[13] Nat'l Acads. Sci., Eng'g, & Med., *Social Media and Adolescent Health* 110 (2024). Problematic use is often seen as a precursor stage to clinical addiction. Nat'l Acads. at 99–100, 108–109; Bar Shutzman & Naama Gershy, *Children's Excessive Digital Media Use, Mental Health Problems and the Protective Role of Parenting During COVID-19*, 139 Computs. Hum. Behav., 107559 (2023); Yunyu Xiao et al., *Addictive Screen Use Trajectories and Suicidal Behaviors, Suicidal Ideation, and Mental Health in US Youths*, JAMA (June 18, 2025), https://doi.org/10.1001/jama.2025.7829 (describing compulsive or addictive use to include feeling unable to stop using a device or platform, experiencing distress when not using it or using it to escape from problems).

[14]Maheux, n.10 *supra*, at 7; Nat'l Acads., n.11 *supra*, at 110-111; *see* Am. Psych. Ass'n, n.12 *supra*, at 7 (recommending "routine" screening of minors for signs of problematic use of social media); *see* Common Sense Media, *A Double-Edged Sword: How Diverse Communities of Young People Think about the Multifaceted Relationship between Social Media and Mental Health* 9 (2024) (nearly half of surveyed minors report control issues with their use of social media, and 63% report taking temporary breaks from social media to address their control issues).

[15]Kaitlyn Burnell, et al., *U.S. Adolescents' Daily Social Media Use and Well-Being: Exploring the role of addiction-like social media use*, Journal of Children and Media 2025, Vol. 19, No. 1, 201 (Table 1), https://doi.org/10.1080/17482798.2024.2402272.

[16] Common Sense Media, *Media Use by Kids Age Zero to Eight* 43–46 (2020); *see also* Bar Shutzman & Naama Gershy, *Children's Excessive Digital Media Use, Mental Health Problems and the Protective Role of Parenting During COVID-19*, 139 Comput.Human Behav., 107559 (2023).

which are not yet fully developed.[17]

A recent study confirms that problematic use behaviors are not limited to only few or uniquely vulnerable minors but are observed in significant numbers among minors across demographic groups.[18] The study finds that over 40% of minors followed from approximately age 10 to age 14 experience increasing or high-peaking addictive use of social media, which includes compulsive use, difficulty disengaging, and distress when not using.[19] The study linked these high and increasing addictive use trajectories to elevated risks of suicidal behaviors and ideation, and worse mental health, including symptoms of anxiety, depression, aggression or rule-breaking.[20]

Studies have also found that personalized, algorithmic engagement feeds are linked with a mental state known as the "flow" state.[21] This state is characterized by "doing something completely concentrated, generating an intense sense of enjoyment and satisfaction, and focusing intensely on the task without being aware of the time."[22] The engagement algorithm enables passive use of a social media platform: a user need not search for content or other users (or even identify categories such as a specific topic or genre). Instead, the platform will automatically select media that the user has never interacted with, including media made by

---

[17] Various neurological mechanisms for how this occurs have been proposed. One hypothesis posits that engagement features trigger the dopamine-producing regions of the brain, and as minors have less-developed abilities to regulate their reactions, the dopamine "bliss" effect is more pronounced. Nat'l Acads., n.11 *supra*, at 50–52. While the mechanisms differ, the underlying causal relationship they attempt to explain does not: minors spending more time online are at increased risk of developing problematic use behaviors. *See* Zhihui Cai et al., *Associations Between Problematic Internet Use and Mental Health Outcomes of Students: A Meta-Analytic Review*, 8 Adolescent Rsch. Rev., 45–62 (2023).

[18] Yunyu Xiao et al., *Addictive Screen Use Trajectories and Suicidal Behaviors, Suicidal Ideation, and Mental Health in US Youths*, JAMA (June 18, 2025), https://doi.org/10.1001/jama.2025.7829.

[19] Yunyu Xiao et al., *Addictive Screen Use Trajectories and Suicidal Behaviors, Suicidal Ideation, and Mental Health in US Youths*, JAMA (June 18, 2025), https://doi.org/10.1001/jama.2025.7829.

[20] *Id.*

[21] Yao Qin et al., *Flow Experience Is a Key Factor in the Likelihood of Adolescents' Problematic TikTok* Use: The Moderating Role of Active Parental Mediation*, 20 Int'l J. Env't Rsch. & Pub. Health 2089 (2023); James A. Roberts & Meredith E. David*, Instagram and TikTok Flow States and Their Association with Psychological Well-Being*, 26 Cyberpsychology, Behav., & Soc. Networking 81 (2023).

*Any trade name used in this document is information provided for the convenience of readers and does not constitute an endorsement of, or opinion regarding, the entity from OAG.

[22] *Id.*

users otherwise unknown to them, in order to keep the feed going.[23] With little to no effort involved, users are more likely to lose track of time when viewing the addictive feed and to be unable to focus on other activities. And because their self-control regulation is still developing, exposure to this kind of engagement is particularly harmful for minors. Minors are, thus, at heightened risk of entering flow states on social media. They have less ability to snap themselves out of the state—and off a social media platform—on their own.

It is, thus, not surprising that minors spend a staggering amount of time on social media. Engagement algorithms are highly effective at increasing the amount of time minors spend on a platform, affecting their ability to leave or focus on other activities. Ninety-five percent of minors aged 13 to 17 use social media, with more than a third reporting that they use it "almost constantly."[24] Fifty-four percent of the same minor users say that it would be hard to stop using social media.[25] According to a nationally representative survey, 8th and 10th graders spend an average of 3.5 hours per day using social media, with 1 in 4 spending 5 or more hours per day and 1 in 7 spending 7 or more hours per day using social media.[26] More than a third of minors aged 8 to 12 have used social media, and nearly 20% report using it daily, which is itself a stunning statistic considering that the largest social media applications have terms and conditions that supposedly prohibit minors under the age of 13 from having accounts.[27]

---

[23]In comparison to engagement features, platform features such as messaging functionality and networking functionality (for example, ability to join and participate in communities) typically are characterized by "active" use such as sending messages and choosing other users to "follow" or "block," and are not associated with negative changes in mental health outcomes. Nat'l Acads., n.11 *supra*, at 75, 106 (2024); *see* U.S. Surgeon Gen. Advisory, *Our Epidemic of Loneliness and Isolation* 20 (2023); *see* Linda Charmaraman et al., *Sexual Minorities and Loneliness: Exploring Sexuality through Social Media and Gender-Sexuality Alliance (GSA) Supports*, Int'l J. Env't Rsch. & Pub. Health 3–5, 11–12 (2024); *see* Matthew Berger et al., *Social Media Use and Health and Well-Being of LGBTQ Youth: Systematic Review*, 24 J. Med. Internet Rsch.12–15 (2022) (compared to non-LGBTQ minors, LGBTQ minors spent more time actively managing settings related to which other users they are able to interact with). Accordingly, the Act's focus on detrimental design features like addictive feeds and nighttime notifications is consistent with the research.

[24] Emily A. Vogels et al., Pew Rsch. Ctr., Teens, Social Media and Technology 2022 (Aug. 10, 2022).

[25] *Id.*

[26] U.S. Surgeon Gen., Advisory, *Social Media and Youth Mental Health* 7 (2023) (citing Richard A. Miech et al., *Monitoring the Future: A Continuing Study of American Youth (8th- and 10thGrade Surveys), 2021,* Inter-university Consortium for Political and Social Research 10 (2022)).

[27] *See* Common Sense Media, *The Common Sense Census: Media Use by Tweens and Teens* 5 (2021); Natasha Singer, *At Meta, Millions of Underage Users Were an 'Open Secret,' States Say*, N.Y. Times (Nov. 25, 2023).

Moreover, a 2025 study of U.S. minors found that 63.8% of minors under the age of 13 had at least one social media account, with this number rising to 70% across all minor age groups.[28]

The more time minors spend online, the more likely they are to experience negative mental health outcomes such as depression, anxiety, and eating and sleep disorders. More time on social media driven by engagement algorithms is linked to a decrease in life satisfaction in minors.[29] According to one study, 12- to 15-year-olds who spent more than 3 hours per day using today's algorithmically driven social media significantly increased their risk of poor mental health outcomes, including symptoms of depression and anxiety.[30] Extensive use is also linked to disordered eating[31,] and low self-esteem.[32] In several random-assignment experiments testing the reduction of use of social media, individuals who reduced their use of or did not use any social media for several weeks were less lonely, depressed, and anxious, and reported being happier than those who did not reduce their user of social media.[33]

Notifications are a different but similarly harmful engagement feature. On most social media platforms, notifications may be sent to a minor at any time of the day by default, including during nighttime. The notification, which includes a visual and possibly also an audio cue, interrupts the minor's current activity with a report of something occurring on the platform. Even if the minor chooses not to engage with the platform in response to a notification, it is disruptive for them to be alerted, read the notification, and decide to act or to

---

[28] Jason M. Nagata *et al.*, *Prevalence and Patterns of Social Media Use in Early Adolescents*, 25 Acad. Pediatrics 7 (2025).

[29] Amy Orben et al., *Windows of Developmental Sensitivity to Social Media*, 13 Nature Commc'ns 1, 5 (Mar. 2022); *see also* Jean M. Twenge & W. Keith Campbell, *Media Use Is Linked to Lower Psychological Well-Being: Evidence from Three Datasets*, 90 Psychiatric Q. 311, 327 (Mar. 11, 2019).

[30] *See* Kira E. Riehm et al., *Associations Between Time Spent Using Social Media and Internalizing and Externalizing Problems Among US Youth*, JAMA Psychiatry (Sept. 11, 2019).

[31] Grace Holland & Marika Tiggemann, *A Systematic Review of the Impact of the Use of Social Networking Sites on Body Image and Disordered Eating Outcomes*, 17 Body Image 100, 108 (June 2016).

[32] *See* Yvonne Kelly et al., *Social Media Use and Adolescent Mental Health: Findings from the UK Millennium Cohort Study*, 6 eClinicalMedicine 59 (Jan. 4, 2019).

[33] Schmidt-Persson et al., *Screen Media Use and Mental Health of Children and Adolescents: A Secondary Analysis of a Randomized Clinical Trial*, JAMA Network Open (2024), doi:10.1001/jamanetworkopen.2024.19881. *See* Hunt Allcott et al., *The Welfare Effects of Social Media*, 110 Am. Econ. Rev. 653-60, 672 (2020); Christopher G. Davis & Gary S. Goldfield, *Limiting Social Media Use Decreases Depression, Anxiety, and Fear of Missing Out in Youth with Emotional Distress: A Randomized Controlled Trial*, 14 Psych. of Popular Media 7-8 (2025); Melissa G. Hunt, *No More FOMO: Limiting Social Media Decreases Loneliness and Depression*, 37 J. Soc. & Clinical Psych. 751, 763 (2018); *see also* Luca Braghieri, Ro'ee Levy, & Alexey Makarin, *Social Media and Mental Health*, 112 Am. Econ. Rev. 3660, 3663 (2022); Hunt Allcott et al., *Digital Addiction*, 112 *Am. Econ. Rev.* 2424-28 (2022).

ignore it.[34] The notification requires the minor's attention and can distract them from other activities. During a typical week, minors as young as 11 routinely receive notifications about a social media feed late at night and into the early hours of the morning when minors are usually sleeping.[35] Disrupted sleep is a significant health issue for minors and is associated with poorer academic performance.[36] It is also associated with other sleep disorders and with mental health issues, including depression, attention/concentration deficiencies, and mood disorders.[37] Notably, minors themselves state they wish it were easier to block notifications and that they wish they had additional support in avoiding them, because the majority of notifications they receive are "spam" notifications they would prefer not to receive.[38]

The mental health effects tied to social media with these engagement features are especially concerning because a minor's neural pathways, which shape their short-term and long-term mental and emotional health, are more vulnerable than an adult's.[39] It is well-established that minors' development and well-being can be seriously affected by external circumstances or stimulation. Thus, changes in a minor's neural pathways caused by hours spent in a "flow state" on an addictive feed, reduction and interruptions in sleep-wake schedules, reduced physical activity and exercise, and reduced opportunities for in-person social interactions—are more pronounced and persist longer than they would in an adult.[40] The Act, accordingly, is protecting the short-term and long-term mental health of minors by targeting these harm-inducing design features.

3. Summary of legislative impetus and legislation

The Legislature passed the SAFE for Kids Act to ensure that millions of New York minors will not be subjected to the risks posed by addictive feeds and nighttime notifications to

---

[34] Common Sense Media, *Constant Companion: A Week in the Life of a Young Person's Smartphone Use* 35 (2023); s*ee* Maheux, n.10 *supra*, at 6–7.

[35] Common Sense Media, *Constant Companion: A Week in the Life of a Young Person's Smartphone Use* 6, 8, 35–38, 43-45 (2023).

[36] Nat'l Acads., n.11 *supra*, at 99-100, 108-109; Sheri Madigan & Stephanie M. Reich, *Consideration of Developmental Stage and the Debate on the Effects of Screens Use—Not All Things Are Created Equal*, 177 JAMA Pediatrics 1123-24 (2023).

[37] Nat'l Acads., n.11 *supra*, at 99-100, 108-109.

[38] Common Sense Media, *Constant Companion: A Week in the Life of a Young Person's Smartphone Use* 6, 32, 35-36, 44, 47 (2023).

[39] Nat'l Acads., n.11 *supra*, at 49–52.

[40] *Id.*

connect with each other and the world through social media. Minors are particularly susceptible to the harms caused by addictive feeds. Many spend hours each day scrolling through social media feeds. The Legislature found that these hours spent on social media have caused harm to New York minors. As detailed in Part II.B.2, minors' time on social media driven by personalized, algorithmic engagement feeds is correlated with mental health harms, including increased rates of depression, anxiety, suicidal ideation, and self-harm.

Through the Act, the Legislature addressed this public health crisis with targeted legislation that balances the diverse interests of minors, parents, online platforms and other stakeholders. The Act prohibits certain websites, online services, online applications, or mobile applications (referred to collectively as "online platforms") from providing minors with an addictive feed that uses data concerning that minor (or the minor's device) to personalize the material the minor sees. At the same time, the Act maintains the operator's ability to moderate media in good faith consistent with their own policies.[41]

The Act covers only those online platforms in which the addictive feed is a significant part of the platform's service and designates such platforms as "[a]ddictive social media platform[s]." [42] Thus, the Act tailors its reach to those operators whose platforms significantly engage in the use of the addictive feeds that harm minors. The Legislature also tailored the Act in such a way as to ultimately encourage parental engagement with their minors' online activities, rather than permanently substitute the government's judgment for a parent's, by allowing minors to seek parental consent to receive an addictive feed.[43]

The Act ensures that minors can still obtain all of the core benefits of covered online platforms and that all New Yorkers will benefit from the Act without compromising their privacy or their experience on covered platforms. With respect to privacy and information security, the law requires that information used to determine age or obtain parental consent must not be used for any other purpose "and shall be deleted immediately after" such use.[44] To ensure continued access to covered online platforms for minors who cannot receive an addictive feed under the law, covered operators may not "withhold, degrade, lower the quality, or increase the price" of their services for those minors.[45] In other words, operators cannot offer inferior services to minors whose parents do not consent to their receiving an addictive feed. If an

---

[41] G.B.L. § 1500(1).

[42] G.B.L. § 1500(2).

[43] G.B.L. § 1501(1)(b).

[44] G.B.L. § 1501(3), (5).

[45] G.B.L. § 1504.

operator allows minors who obtain parental consent for an addictive feed to use the platform, it must allow minors who do not obtain parental consent to also access the platform but without an addictive feed or an otherwise degraded experience.

The harmful engagement features targeted by the Act are separable from other features of online platforms like content creation, content moderation, user choices on engagement or privacy settings, messaging, networking, and searching. Covered operators' ability to provide and minors' ability to use those other features is in no way impeded by the Act. Under the Act, a feed is not an addictive feed if it is based on a) "user-selected privacy or accessibility settings, or technical information concerning the user's device;" b) express and unambiguous requests for "specific media, media by the author, creator, or poster of media the user has subscribed to, or media shared by users to a page or group the user has subscribed to;" or c) requests to block, prioritize, or deprioritize, such media. The Act is also clear that where the media is "direct, private communications," search results, or the "next in a pre-existing sequence," it is not an addictive feed.[46]

The Legislature also found that overnight notifications presented a public health risk. The Act therefore prohibits social media platforms from sending "notifications concerning an addictive feed" to a known minor between 12 AM Eastern and 6 AM Eastern without obtaining parental consent.[47]

The Legislature has charged OAG, which has significant experience with the harms of social media, privacy, and complex technical issues through its investigations and litigation, and through its in-house research and analytics team, with promulgating regulations before the statute can go into effect. Covered online platforms are required to use "commercially reasonable and technically feasible methods" to determine if a covered user is a minor before providing them with an addictive feed. The OAG is charged with promulgating regulations identifying such commercially reasonable and technically feasible methods, taking into consideration a number of factors.[48] If a user is a minor, the social media platform must obtain "verifiable parental consent" before providing the minor with an addictive feed. The OAG is also charged with promulgating regulations identifying methods of obtaining verifiable parental

[46] G.B.L. § 1500(1).

[47] G.B.L. § 1502.

[48] G.B.L. § 1501(1)(a), (2).

consent[49] and any needed language access regulations.[50] In addition, OAG has authority to promulgate regulations to effectuate and enforce the Act as a whole.

The Act goes into effect on the 180th day after OAG promulgates rules and regulations necessary to implement the Act.[51]

III. Needs and Benefits

A. Section 700.1 Definitions

This section explains the definitions in the proposed rule. The OAG carefully reviewed and considered comments in response to the Advanced Notice of Proposed Rulemaking issued on August 1, 2024 ("ANPRM"), in proposing the definitions and in this Regulatory Impact Statement. While some explanations of definitions specifically note aspects of the proposed rule on which OAG seeks comment, OAG seeks, requests, and welcomes comments and the submission of data on all aspects of the proposed rule, including the definitions in section 700.1.

1. Accredited Third-Party

The proposed rule defines "accredited third-party" to mean a person qualified to certify an age assurance method, as determined by the American National Standards Institute or an equivalent accreditation body, using the accreditation standard from the International Organization for Standardization and International Electrotechnical Commission ("ISO/IEC") 17065:2012: Conformity assessment — Requirements for bodies certifying products, processes and services ("ISO 17065"), or an equivalent industry standard. Requiring age assurance methods to be certified only by accredited third-parties further strengthens the integrity and uniformity of the testing and certification process.

Because the data minimization and deletion requirements in G.B.L. § 1501 reduce the amount of data regarding covered operators' application of age assurance that is available for analysis and audit, the process of testing and certifying an age assurance method, both initially and annually thereafter, takes on particular importance in ensuring covered operators are offering effective age assurance methods that adhere to the obligations of the proposed rule. Accordingly, OAG has specified that certification take place in accordance with established industry standards and has further specified additional testing and test data parameters.

---

[49] G.B.L. § 1501(1)(b), (4).

[50] G.B.L. § 1506.

[51] L. 2024, ch. 120 § 5.

Additionally, by requiring accreditation for the persons performing the testing and certification, OAG intends to allow testing to be carried out only by persons with the appropriate capacity, tools, and testing frameworks. This requirement increases confidence in the testing and certification process, and by extension in age assurance methods themselves.

The specification that the accredited person be a "third-party" is intended to make clear that, except as specified in section 700.5(f), testing and certification should be performed by a person unaffiliated with the covered operator. The ISO 17065 accreditation process requires a lack of bias with respect to the testing entity and the subject. Presumably any robust industry standard would include a similar requirement. Once again, this ensures fairness in the testing and certification process and protects the perception of that process by users and the public.

2. Accuracy Minimum

The proposed rule defines the term "accuracy minimum" to mean the acceptable level of accuracy for an age assurance method, measured as a series of age-specific false positive rates, along with a 98% detection rate for method circumvention. Setting a different false positive rate for each of five age brackets (ages 0 to 7, ages 8 to 13, ages 14 to 15, age 16, and age 17) reflects the intersection of the policy goal of the statute, to protect minors from the mental health harms of addictive feeds and nighttime notifications, with the Legislature's interest in ensuring that goal is pursued in a commercially reasonable and technically feasible way. The OAG seeks comment on the definition of the accuracy minimum.

Many age assurance methods are highly effective at confirming minor age status for young children. It can be more difficult to determine whether a user is a minor as the minor approaches 18. This is true even for methods with high accuracy rates overall. For example, facial age estimation technology is nearly 100% effective in determining that children aged 8 to 13 years of age are minors under 18. The same technology is less effective in determining whether a 17-year-old is over or under 18.

After careful review and consideration of the effectiveness of various age assurance methods together with information gathered through the ANPRM process and outreach to and from various stakeholders, OAG proposes allowing covered operators to use methods that have false positive rates as follows: a maximum of .1% for minors aged 0 to7, 1% for minors aged 8 to 13, a maximum of 2% for minors aged 14 to 15, a maximum of 8% for minors aged 16, and a maximum of 15% for minors aged 17. Allowing slightly reduced accuracy rates for users as they get closer to adult status will protect more of the youngest minors while still protecting the substantial majority of older minors and providing operators with robust options for age assurance that are commercially reasonable and technically feasible. Allowing for a wider variety of commercially reasonable and technically feasible age assurance methods to meet the accuracy minimum also allows covered operators to facilitate user choice of age assurance methods and to minimize associated burden.

Generally, in calculating the accuracy minimum, the proposed definition would require a covered operator to count all false positives—or minors that are wrongly identified as adults—as part of the accuracy minimum. However, the proposed definition of accuracy minimum excludes two categorical outcomes from the calculation following the initiation of age assurance for a covered user: 1) where the covered user fails or refuses to provide all information requested by the covered operator and thereby essentially fails to complete the process and 2) inconclusive age assurance outcomes, which are defined in section 700.1(t), as an outcome in which the covered operator is unable to reach a conclusion regarding the user's age status, typically because the data used by the operator, including data submitted by or otherwise collected from the user, fails to meet a quality threshold required for the age assurance method to function as intended. Both exclusions recognize that the accuracy of an age assurance method is dependent upon user inputs. A user's failure to make essential data available, or a user's good faith provision of data that is not of sufficient quality, should not adversely impact an age assurance provider's ability to meet the accuracy minimum. At the same time, inconclusive age assurance outcomes are included in the total accuracy minimum, for the reasons set forth in the explanation of that definition as well as of inconclusive age assurance. The accuracy minimum also does not address false negatives for the reasons set forth in the explanation of that definition.

The OAG considered alternative accuracy minimums, including a single accuracy minimum that would apply across all ages as well as higher and lower accuracy minimums for the age groups. The OAG based the proposed accuracy minimums on the most up-to-date information and data available on age assurance. As described in Part III.D, interest in age assurance, age assurance technology, and related public information are rapidly growing and evolving and OAG may revise the accuracy minimum in the future to reflect technological improvements. The OAG preliminarily concludes, consistent with the economic analysis in Part IV and the discussion of age assurance technology in Part III.D, that the proposed accuracy minimums reflect a commercially reasonable and technically feasible standard for covered operators.

Also included in the accuracy minimum is a 98% rate of detection of method circumvention. Effective age assurance methods must include tools to identify and reject all varieties of method circumvention and must continually evolve those tools to combat new and increasingly sophisticated attack methods. Including a minimum rate of detection, which will be measured as part of the testing and certification process in accordance with section 700.5(b)(4), ensures that covered operators will offer age assurance methods that can effectively detect method circumvention, at which point the covered operator can take appropriate action, including requiring submission of accurate user data and, in the absence of prompt compliance, defaulting to assuming minor status for the covered user.

3. Addictive Feed

The proposed rule defines the term addictive feed consistent with the definition in the Act with minor changes or additions for clarity. In G.B.L. § 1500(1), addictive feed means an online platform or portion thereof in which "multiple pieces of media generated or shared by users" to an online platform are "recommended, selected, or prioritized for display based, in whole or in part, on information associated with the user or the user's device." The OAG seeks comment on the proposed definition of addictive feed.

In section 700.1(hh), the proposed rule defines "user" as any person other than the operator, its agents, or its affiliates. Furthermore, in section 700.1(dd), the proposed rule defines "person" to include individual or natural persons as well as any form of business enterprise. Thus, one component of an addictive feed, is that a stream, feed, or other presentation must include media that is not generated by the covered operator or platform, but by third-parties, whether they are members of the general public sharing personal photos, businesses advertising their products, or sophisticated users creating and posting media to influence other users, gain a following, or for any other reason. The Act and proposed rule treat all users and media equally. Neither the nature of the user nor the reason the user generated or shared the media would change the application of the Act and this proposed implementing rule.

To be an addictive feed also requires the recommendation, selection, or prioritization to be based on information associated with the user or the user's device. This mechanism, where a user receives media based on information associated with that user, is often referred to as personalization with multiple pieces of such media presented based on this mechanism often called a "personalized feed." The proposed rule incorporates the phrase "multiple pieces of media" as well as the reference to media being provided "concurrently or sequentially" from the statute. An addictive feed, thus, includes many different ways in which personalized, user-generated media is displayed to a user. For example, a platform may use a continuous or user initiated scroll of multiple pieces of personalized media, with one or more pieces of media on the user's screen at any given time. Another option would be for the operator to include multiple pieces of personalized media arranged on one screen to be viewed concurrently or sequentially. There are many possible permutations, including multiple feeds on a single display.

In G.B.L. §§ 1500(1)(a) through (h), the statutory definition includes seven "conditions" which, if met individually or in combination, exclude what would otherwise be an addictive feed or personalized feed from the definition. Proposed section 700.1(c)(3) tracks the definition and exclusions with certain clarifications for ease of compliance.

The proposed rule incorporates G.B.L. § 1500(1)(a) into the affirmative definition of addictive feed to provide a more streamlined definition. In G.B.L. § 1500(1), an addictive feed is characterized by presenting media based on "information associated with the user or the user's device." Under G.B.L. § 1500(1)(a), however, if the recommendation, prioritization, or selection of media to the user "is based on information that is not persistently associated with the user or

the user's device" and "does not concern the user's previous interactions with media generated or shared by other users," it is not an addictive feed.

Thus, the proposed rule defines addictive feed as "an online platform, or a portion thereof, in which multiple pieces of media from an online platform are: 1) shared or generated by users, and 2) concurrently or sequentially, recommended, selected, or prioritized for display to a user based, in whole or in part, on (i) information persistently associated with the user or the user's device; or (ii) the user's previous interactions with media generated or shared by other users including the user's interactions on different online platforms media or the pages, groups, or other user-generated media the user requests, subscribes to, otherwise selects or a combination thereof."

In so combining the definition and first condition, the proposed rule clarifies that the use of information associated with the user is a necessary but not sufficient basis for a feed to be an addictive feed. Instead, the information used to create the personalized feed must be either, information persistently associated with the user or the user's device or reflect the user's previous interactions with media generated or shared by other users. Proposed section 700.1(u) defines information persistently associated with a user to provide covered operators with further guidance on personalization that qualifies as an addictive feed under the proposed rule.

Additionally, consistent with the Act, which states a feed is not an addictive feed if it does not concern the user's interactions with media generated or shared by other users, the proposed rule clarifies that previous interactions with media generated or shared by other users may include data about how a particular user interacts with user-generated media across the user's device or use of online platforms—rather than being limited to the user's interactions with user-generated media on the one online platform the user is on. Operators regularly use data and information they collect across a user's device or interactions on different online platforms.[52] This data can facilitate the same kind of personalization, and thus, harms, as information tied to a particular platform.

The proposed rule includes the other conditions in the Act under which recommendation, selection, prioritization, or display of media is not addictive feed. The proposed rule clarifies that these particular displays of media are not an addictive feed. Notably, rather than information the platform associates with the user and uses to algorithmically recommend, select, or prioritize user media, these conditions are based on a user's affirmative actions.

---

[52] *See, generally* Federal Trade Commission, *Commercial Surveillance and Data Security Rulemaking*, Aug. 11, 2022, https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking.

First, section 700.1(c)(3)(i) clarifies that recommending, selecting, or prioritizing media based on user-selected privacy or accessibility settings or technical information related to the user's device is not an addictive feed. The proposed rule does not intend to override user privacy and accessibility choices or to render an online platform inaccessible based on necessary, device-specific technical information. Such information might include information about the device's operating system or general location information allowing the covered operator to determine whether the device is being used in the State of New York. The proposed rule also defines technical information concerning the user's device in this section 700.1(ff).

Similarly, the Act and proposed rule, sections 700.1(c)(3)(ii)-(iv), do not intend to frustrate or disrupt responses to user requests for or to avoid media by an author based on express and unambiguous requests or subscriptions to either specific users, authors, creators, groups, posters, or a particular page. This includes media by a friend or family member. It also includes media posted by users to an interest group. For a covered minor user who subscribes to a group and does not have parental consent for addictive feeds, the covered operator cannot use information persistently associated with the user or with the user's interactions with other media to recommend, select, or prioritize media from the group the user subscribes to. It can, however, deliver that media to the covered minor.

Under section 700.1(c)(3)(vi), a covered operator may also recommend, select, or prioritize media in response to a user search inquiry. Consistent with the statute, the proposed rule does not intend to change the mechanism by which covered operators display media in response to search inquiries. The proposed rule also mirrors the statute in explicitly stating that a covered operator may provide minors access to direct and private communication without consent; again, the proposed rule does not intend to cover this mechanism, which connects persons to each other. The statute and proposed rule also clarify that a covered operator may display media based on media that is next in a pre-existing sequence and that a covered operator may recommend, prioritize, or select information necessary to comply with the proposed rule and any other related regulations.

4. Addictive Online Platform

The proposed rule defines "addictive online platform" to mean an online platform that "offers or provides users an addictive feed as a significant part of the services provided." G.B.L. § 1500.1(2). In the preamble of the Act, the Legislature stated that this definition reflected its decision not to prohibit addictive feeds "on online services that provide such feeds as ancillary features or add-ons, or where users are on the feed for a relatively small portion of their time using the service."

First, the proposed rule clarifies that an addictive online platform may consist of multiple addictive feeds that jointly comprise a significant part of the online platform. For example, a platform may consist entirely of addictive feeds with the feeds separated into 10 different addictive feeds, including with one related to sports, one related to health, one with pet-based

media, and other topic specific feeds. Under the proposed rule, that online platform would be an addictive online platform with the potential to cause the same mental health harms to minors.

To facilitate compliance, the proposed rule also includes an objective metric to determine whether addictive feeds are a significant part of an online platform. Under the proposal, online platforms for which twenty percent or more of total monthly active user time, as measured over a period of six months in the prior calendar year, is spent on addictive feeds are addictive online platforms. As it is not clear that a particular six-month period would be more representative than another, OAG allows covered operators the flexibility to choose a six-month period in the prior calendar year. The OAG considered a number of alternative options but preliminarily finds that this metric will most closely reflect the legislature's intent to cover those platforms for which the addictive feeds are a significant component.

While online platforms with addictive feeds track many metrics to determine their effectiveness or performance, different measures of user time and attention are important for platforms that use addictive feeds. As noted in Part IV, user time and attention are often tied to the ability of a platform to monetize. Oft-quoted metrics measuring user time and attention include the number of daily active users or monthly active users, although online platforms often calculate these metrics differently.[53] The number of user-generated posts or measures of user "engagement," such as likes or click-throughs, are also generally calculated.

The OAG proposes user time on the addictive feed as a percentage of total user time as a metric because OAG understands that online platforms generally track user time spent on various parts of their platform, including addictive feeds. Monthly active user time for these purposes reflects time spent in an active session or visit to the online platform, which is a continuous interval in which the online platform is available for user input and the user initiates

---

[53] *See, e.g.,* Meta Platforms, Inc., Annual Report (Form 10-K) Jan. 29, 2025 (explaining calculation of Daily Active people in 2024), https://www.sec.gov/Archives/edgar/data/1326801/000132680125000017/meta-20241231.htm;: (explaining calculation of Daily Active people in 2024 10-K for Meta); Pinterest, Inc., Annual Report (Form 10-K), Feb. 6, 2025 (explaining calculation of Monthly Active Users in 2024 10-K for Pinterest); Reddit, Inc., Annual Report (Form 10-K), Feb. 12, 2025, https://www.sec.gov/ix?doc=/Archives/edgar/data/0001713445/000171344525000018/rddt-20241231.htm#ib99e0360e0fc4ee093fa01d97bc4a43c_10 (explaining calculation and use of Reddit's two different metrics DAUq and WAUq, daily active unique user and weekly active unique user).Feb. 6, 2025 (explaining calculation of Monthly Active Users in 2024 10-K for Pinterest), https://s204.q4cdn.com/3694585 https://s204.q4cdn.com/369458543/files/doc_financials/2024/q4/973659c6-d9a4-483b-a151-22b4a2a5bd9e.pdf 43/files/doc_financials/2024/q4/973659c6-d9a4-483b-a151-22b4a2a5bd9e.pdf; Reddit, Inc., Annual Report (Form 10-K), Feb. 12, 2025 (explaining calculation and use of Reddit's two different metrics DAUq and WAUq, daily active unique user and weekly active unique user), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001713445/000171344525000018/rddt-20241231.htm#ib99e0360e0fc4ee093fa01d97bc4a43c_10.

at least one interaction event, such as clicking, scrolling, commenting, or sharing content, during the session.

The OAG did not propose the number of users of the addictive feed as a portion of all users of the platform, although this may also reflect the extent to which the addictive feed is significant. The OAG preliminarily concludes that the number of users may not be as accurate in measuring whether the addictive feed is a significant part of the whole platform. For example, users might all briefly visit a feed but spend nearly all of their time elsewhere on the platform. The OAG seeks comment on the use or addition of a metric measuring the relative number of users of the addictive feed as part of the definition of addictive online platform.

The OAG also considered whether revenue attributable to the addictive feed as a portion of the online platform's total revenue should be a factor in this definition. However, as Part IV explains, historically, a large number of users spent significant time on the addictive feeds of the largest online platforms before those platforms were able to monetize the number of users and their time spent. The OAG preliminarily concludes that even if an online platform is able to monetize the addictive feed when a relatively small amount of time is spent on the addictive feed by users, that revenue may not be the best measure of whether the addictive feed is a significant part of the platform for purposes of the law.

Having preliminarily concluded that time spent may be the most appropriate and measurable metric to determine whether an addictive feed is a significant part of the platform, OAG considered what portion of time on an addictive feed is significant. Based on its understanding of the market and its expertise, OAG proposes 20% of time spent. As an initial matter, significant means "embodying or bearing some meaning."[54] To be a significant part does not mean the addictive feed must be the largest or most important component—it must, however, as the Legislature stated, be more than "ancillary" or an "add-on."

The OAG preliminarily concludes that if 20 percent or one fifth of user time overall is spent on the addictive feed, this is significant from the perspective of an operator of an online platform. The OAG also preliminarily concludes that if the addictive feed is where 20 percent of user time is spent, whether 100 percent of user time for some users adds up to 20 percent of the total, or each user spends 20 percent of their time on the additive feed, the addictive feed is a significant part of the online platform. Excluding exempt addictive online platforms from coverage by the proposed rule also means that an online platform will only be required to comply with the proposed rule when it is large enough that 20 percent of the time spent on its platform will translate to significant total time spent on the addictive feed.

---

[54] SIGNIFICANT Definition, Black's Law Dictionary (12th ed. 2024).

The OAG seeks comment and data related to the standard in the proposed rule or alternative definitions.

5. Adult

The proposed rule defines the term "adult" to mean an individual 18 years old or older. The term provides the counterpart to the statutory definition of "minor" provided in G.B.L. § 1500(6) and allows for greater clarity in other provisions in the proposed rule.

6. Affiliate

The proposed rule defines the term affiliate to mean any person that directly, or indirectly through one or more intermediaries, controls, is controlled by, or is under common control with the person specified. This definition is consistent with the commonly understood legal meaning of affiliate[55] and other regulatory definitions of affiliate under New York law.[56] The OAG seeks comment on the proposed definition of affiliate.

7. Age status

The proposed rule defines "age status" to mean the state of being either 18 years old and over (an adult) or under 18 years old (a minor). Knowledge of age status does not require knowledge of an individual's exact age. For example, an operator may only learn that an individual is an adult, without also learning the individual's birthdate or that the individual is a certain number of years old. This term is not defined in the statute but is defined here to facilitate defining accuracy minimum and total accuracy minimum in addition to the requirements under sections 700.3 and 700.4. Allowing covered operators to use age status, rather than requiring the specific age of a user, allows operators to comply with the proposed rule in a more privacy and data security protective way.

8. Age Assurance Method

The proposed rule defines "age assurance method" as any type of age estimation, age inference, or age verification. "Age assurance" is typically used as an umbrella term for various types of methods that can support a conclusion regarding an individual's age or age status, often for the purpose of making an age-related eligibility decision. For purposes of compliance with the proposed rule, OAG has identified three categories of age assurance that are considered age assurance methods, each of which contains one or more methods that can meet

---

[55] Black's Law Dictionary (12th ed. 2024) (defining affiliate to mean "[a] corporation that is related to another corporation by shareholdings or other means of control; a subsidiary, parent, or sibling corporation.")

[56] *See, e.g.*, 13 N.Y.C.C.R. § 12.3 (similarly defining affiliate in rules governing Article 16 of the Business Corporation Law); *see also* 3 N.Y.C.C.R. § 322.6 (similarly defining affiliate for purposes of banking law).

the accuracy minimum if effectively implemented and executed. The OAG seeks comments on the proposed definition of age assurance method.

Under the proposed rule, self-declaration is not an age assurance method. However, self-declaration as a minor qualifies a covered user as a covered minor for purposes of compliance with section 700.4. Allowing minors to self-declare their minor age status is consistent with the legislative intent of the Act to protect minors from addictive feeds and nighttime notifications and would reduce the amount of information operators collect to comply with the proposed rule and, thus, allow for compliance in a more privacy and data security protective way for minors.

An age assurance method would be required for all covered users who do not self-declare as minors. By proposing to define age assurance method through categories of methods rather than specific methods, OAG would allow covered operators to determine the method or methods that are best suited to the online platform and users. It also would allow operators to remain flexible in choosing methods as age assurance methods and technology continue to evolve. The accuracy minimum and requirements of section 700.4 ensure that the methods operators ultimately choose are effective.

For a covered user that is a business entity of any kind, the proposed rule requires the covered operator to conduct an age assurance method for at least one individual with actual authority from the entity. If the individual is deemed to be an adult by an age assurance method meeting the accuracy minimum, the user's account may be given adult status pursuant to section 700.2(a)(1). This level of screening, which is only minimally burdensome to the entities, ensures minors do not evade the law by creating accounts in the name of business entities.

9. Age Estimation

The proposed rule defines "age estimation" to mean an age assurance method that determines the age or age status of a covered user by analyzing a physical feature or attribute for that user. Examples include facial age estimation, voice age estimation, and age estimation via hand movements. Age estimation involves the application of machine learning to data provided by a covered user, which may be captured or requested as an uploaded image, video, or audio sample. The machine learning does not need to identify the user; rather, the user's age or age status can be the only necessary information determined and reported. Age estimation also may include a "liveness" check or other features designed to detect the submission of false information.

10. Age Inference

The proposed rule defines "age inference" to mean an age assurance method that determines the age or age status of a covered user using one or more documented facts that, while not directly confirming the covered user's age or age status, allow age or age status to be deduced with enough statistical accuracy to meet the accuracy minimum. Examples include

email age inference (i.e., checking a user's email address against data sources to detect indicia of adulthood, such as association with a mortgage or utility bill), analysis of documents such as mortgage statements, utility bills, or college transcripts, and analysis of a covered user's past behavior on the covered operator's platform. To qualify, the authenticity of the information must be verified and confirmed to be associated with the covered user. The covered user may or may not be alerted to the use of age inference for determination of the covered user's age or age status, depending upon whether the covered operator already has the necessary information and user consent.

The OAG seeks comments on the proposed definition of age inference.

11. Age Verification

The proposed rule defines "age verification" to mean an age assurance method that determines the age or age status of a covered user by reviewing a generally accepted form of identification, most commonly government-issued identification, which lists the age of the covered user, or validates the covered user's age or age status against a verified records source such as a government agency record or a consumer credit bureau. The OAG seeks comments on the proposed definition of age verification.

Consistent with the requirements of the Act, the inclusion of age verification as an allowable category of age assurance methods in the proposed rule is subject to the requirement that a covered operator offer at least one alternative age assurance method that does not require the furnishing of government-issued identification, unless that covered operator already possesses the government-issued identification to comply with other laws. Alternatively, the covered operator may offer age verification in the form of zero-knowledge proof age assurance, as defined in the proposed rule. Both measures are designed to ensure that age verification is performed in a manner that maximizes privacy protections and data security for the covered user.

Because not all covered users have government-issued identification, OAG also proposes mandating that covered users who are asked to provide government-issued identification and decline to do so be allowed to proceed to the appeals process as set forth in section 700.6. This ensures that any covered user who claims to have adult status but does not complete age verification via government-provided identification may, at a minimum, confirm that adult status by presenting information through the appeals process. Such user also may confirm adult status through the completion of an alternative age assurance method such as age estimation or age inference, if offered by the covered operator.

12. Certification

The proposed rule defines "certification" as the confirmation by an accredited third-party that an age assurance meets three important benchmarks. The first is an industry standard for effectiveness, applying either ISO/IEC 27566:2025: Information security, cybersecurity and

privacy protection — Age assurance systems ("ISO 27566"),[57] the Institute for Electrical and Electronics Engineers 2089.1 Standard for Online Age Verification ("IEEE 2089.1"), or an equivalent industry standard. The second is confirmation that the age assurance method meets the accuracy minimum. Additionally, the accredited third-party must specify whether the age assurance method meets the total accuracy minimum, *see* section 700.5(b)(7), although meeting the total accuracy minimum is not a requirement for certification. The third and final requirement is confirmation that the accuracy method has undergone the testing requirements in 700.5(b), which, in addition to the false positive rates that underlie the accuracy minimum, also include testing metrics such as false negative rates, detection of method circumvention, and data collection, segregation and deletion measures, among others. While a number of these metrics may be covered by the applicable industry standard, OAG chose to specify testing that is critical to the integrity of the age assurance method.

Of particular note, to the extent that an age assurance method offers variable settings or options, certification is limited to only the settings or options employed during testing, *see* section 700.5(e). The purpose of this requirement is to prevent covered operators from diverging from the conditions that generated the test results enabling certification, which would undermine the accuracy minimum requirements and other aspects of testing.

13. Covered minor

The proposed rule defines "covered minor" as it is defined in the statute to mean a user of an online application in New York for whom the covered operator has actual knowledge the user is a minor.

14. Covered Operator

The proposed rule defines "covered operator" to mean any person who operates or provides an addictive online platform consistent with G.B.L. § 1500.7. The proposed rule additionally clarifies that any agent or affiliate of a covered operator is a covered operator if they are involved in operating or providing an addictive online platform. Such agents or affiliates are not covered users under the statute and the proposed rule.

15. Covered user

The proposed rule defines "covered user" a user of an online platform in New York, not acting as an operator, or agent or affiliate of the operator of such online application or any portion thereof, consistent with G.B.L. § 1500.4. The OAG seeks comments on the proposed definition of covered user.

---

[57] The ISO 27566 standard is in final draft form and expected to take effect prior to the effective date of the proposed rule. *See* https://www.iso.org/standard/88143.html.

An operator (or its agents or affiliates) may have public-facing corporate user accounts on its online application that visually are similar or even identical to accounts belonging to unaffiliated users, but such accounts would not make the operator a user under the statute or proposed rule. "Agent" has the meaning granted it by existing New York State law and "affiliate" is defined in section 700.1(f). A third-party is not an "agent" or "affiliate" of an operator solely on the basis of a monetary transaction between the third-party and the operator. For example, if a third-party contracts with the operator (or its agent or affiliate) to create and post media on the third-party's behalf, the third-party is a user of the online platform, and the media posted on the online platform on the third-party's behalf is generated by a user under the proposed rule.

16. Delete

The proposed rule defines "delete" as to permanently destroy, remove or deidentify information, using reasonable measures to protect against the unauthorized access or use of such information and to ensure that such information may not be retrieved after the deletion process has been completed. G.B.L. §§ 1501.3 and (5) impose obligations on a covered operator to "immediately" delete information collected about a user for purposes of complying with the Act. The OAG proposes this definition to clarify a covered operator's related obligations and seeks comment on the proposed definition.

Under the proposed rule, de-identifying information may constitute deletion, provided that it meets the stringent requirements in the proposed rule. The proposed rule sets forth that any covered operator choosing a de-identification process must: (1) take reasonable measures to de-identify any information that identifies or can reasonably be linked to an individual or device; (2) take reasonable measures to ensure the de-identified information cannot be re-linked with an individual or device; (3) not process and must publicly commit not to process the de-identified information except only in its de-identified state, and must not attempt to and must publicly commit not to attempt to re-identify or re-link the de-identified information; (4) take reasonable measures to ensure any recipients of de-identified information also abide by these restrictions; and (5) take reasonable measures to ensure that the de-identified information is only retained as long as necessary to fulfill the purposes permitted under the rules implementing the Act, and is not used for any other purpose.

Accordingly, a covered operator may use de-identification processes if information cannot be re-linked to other information that would make the records whole again. Such requirements balance user privacy and security with technical and operational flexibility for operators. Furthermore, allowing for de-identification with stringent requirements is consistent with state laws setting forth commercially reasonable and technically feasible standards for online and digital data destruction, which have generally been accepted across many different

industries without issue.[58] The OAG would expect covered operators choosing to de-identify information to comply with the proposed rule to continually monitor best practices for de-identification processes. To be clear, if an operator fails to adequately de-identify information according to the requirements set out in the proposed rule, the operator is not complying with the Act.

17. Exempt Addictive Online Platform

The proposed rule defines "exempt addictive online platform" to mean an addictive online platform that meets at least one of two criteria: 1) fewer than 5,000,0000 global monthly active users; or 2) fewer than 20,000 covered minor users. These criteria represent a threshold below which compliance with the proposed rule is not commercially reasonable and technically feasible as determined by OAG, consistent with the accompanying economic analysis.

The exclusion would not apply to addictive online platforms whose primary user base is minors because excluding the users of those platforms would not be consistent with the statute's goal of protecting minors from addictive feeds. Moreover, a new online platform whose primary user base is minors that is entering the market and relies on addictive feeds must be prepared to comply with the law and may, thus, avoid offering addictive feeds as a significant part of their online platforms. Finally, such a platform presumably would avoid conducting age assurance methods on most of its users because the platform can designate users as covered minors through self-declaration. The OAG seeks comments on the proposed definition of exempt addictive online platform.

For the first criterion, based upon information from industry experts and data from existing platforms, OAG preliminary finds that addictive online platforms with fewer than 5,000,000 global monthly active users are receiving less revenue from advertising and/or other types of user fees, both overall and on a per-user basis, and their user turnover rates are higher than larger platforms. As described in Part IV, due to higher user turnover, the costs of age assurance methods are higher based on the rate of new user onboarding as a percent of all users. Thus, the costs of age assurance methods are a larger percentage of the covered operators' overall costs and expenses as compared to a platform with 5,000,000 or more monthly active users.

Further, due to the lower overall and per-user revenue, smaller operators are less able to generate revenue to offset the costs of age assurance methods versus larger platforms. Similarly, as described in Part III.D, implementing reliable age assurance methods that meet the

[58] *See, e.g.*, California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.140(m) and Cal. Code. Regs. tit. 6, § 7022(b)(1); Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1303(11) and Colo. Code. Regs. 4 § 904.3-4.06; Rhode Island Data Transparency and Privacy Protection Act, R.I. Gen. Laws § 6-48.1-2(13) and 6-48.1-7(j), (n) (effective Jan. 1, 2026).

accuracy minimum is technically feasible and as noted in Part IV, it is feasible at a reasonable cost. The OAG preliminarily finds that to be technically feasible and commercially reasonable in the market of covered operators, operators need a minimum of 5,000,000 users.

With respect to the second criterion, for online platforms with 20,000 covered minor users, constituting less than one percent of the corresponding population of minors in the State of New York, OAG preliminarily finds that age assurance method costs are not commercially reasonable at the otherwise technically feasible accuracy minimum when compared to the modest benefit to the covered operator of maintaining this small number of users in New York. Allowing exemption from compliance with the proposed rule on this basis therefore incentivizes operators to offer services to users in the State of New York, including covered minors, without bearing the costs of age assurance methods that complies with the proposed rule until such time as doing so becomes commercially reasonable. Moreover, this exemption is consistent with the Legislature's intent to balance protection for minors with commercially reasonable measures for age assurance methods.

The proposed exemption from compliance with the proposed rule for addictive online platforms meeting at least one of the above criteria ensures that age assurance methods will be required only at such time as it is commercially reasonable and technically feasible for the covered operator. The proposed exemption allows for the Legislature's intent of facilitating a healthy market, including for operators looking to launch new platforms or expand existing platforms into the State of New York. Once the applicable exemptions no longer apply to the covered operator, that covered operator must meet all requirements in the proposed rule within 180 days. Covered operators who operate an online platform qualifying as an exempt addictive online platform after originally not meeting either criteria, through the loss of either monthly active users or covered minors, also do not need to comply with the requirements of the proposed rule until such time as their monthly active user or covered minor user numbers once again exceed the thresholds allowed by the exempt addictive online platform definition, at which time they must come back into compliance within 30 days.

18. False Negative

The proposed rule defines "false negative" to mean incorrectly identifying an adult as a minor. False negatives are not a component of the accuracy minimum, which measures only instances in which a minor is incorrectly identified as an adult. In addition, where a false negative outcome is reached following an age assurance method, the covered user would have an automatic right to an appeal, pursuant to section 700.6.

The OAG recognizes that false negatives may create some burden for covered users who are incorrectly identified as minors and must then take additional steps, via the appeals process, to present additional evidence of adult age status. The OAG believes that based on current age assurance technology, age assurance methods are available that minimize false negatives. Further, covered operators are commercially incentivized to minimize burden on covered users.

The proposed rule does not specify an allowable false negative rate because the OAG believes market forces, including competition based on user friction, will create sufficient incentives to minimize it. The OAG notes that covered operators should take into account the impact of false negative rates on different categories of users.[59] Accordingly, OAG proposes that false negative rates be measured as part of the certification process in section 700.5, thus ensuring that operators are aware of, and can minimize, the false negative rates associated with the age assurance methods they choose to offer.

The proposed rule also includes language directing covered operators to take steps to minimize false negative outcomes by acting reasonably and in good faith to adopt age assurance methods with lower false negative and false positive rates in accordance with industry developments. This directive is designed to ensure covered operators optimize outcomes for users as the availability and accuracy of age assurance technology continues to improve.

19. False Positive

The proposed rule defines "false positive" to mean incorrectly identifying a minor as an adult. Before offering an age assurance method, covered operators must ensure that the false positive rates of that method do not exceed the allowable false positive rates set forth in the accuracy minimum. False positive rates must be established by the certification process set forth in section 700.5.

20. Inconclusive Age Assurance Outcome

The OAG proposes defining "inconclusive age assurance outcome" to mean the determination by a covered operator, following submission of all requested information by the covered user, that the user's age status cannot be provided using the selected age assurance method engaged. It is expected that this outcome generally will occur when a covered user submits low-quality data or data that otherwise cannot be used to process the age assurance method, thus, not allowing the age assurance method to function effectively. It also may result from an age assurance method that is tuned to be too sensitive to lower quality data. An inconclusive age assurance outcome is limited to a good faith data submission by a covered user and is distinct from an instance in which a covered user intentionally submits data in an attempt to generate a false positive result from the age assurance method. The latter should be treated as a false positive result (if the age assurance method is completed and a false positive result is rendered) or a failure to complete the age assurance method (if the age assurance method is not completed).

For example, a covered operator might use email verification as an age assurance method. The method may meet the accuracy minimum when provided an email address for

[59] *See, e.g.,* Human Rights Law § 296.

which the method has sufficient data to confirm adult status. However, when a covered user who is an adult and has a new email address submits their email address, the result will be an inconclusive age assurance outcome. In that instance, the covered user submitted the information requested during the age assurance process, but the method could not determine the age status of the user. Another example of an inconclusive age assurance outcome might occur when a covered operator offers facial age estimation that meets the accuracy minimum and a covered user using a laptop to access a platform makes an effort to go through the process but has a laptop camera with low quality. If the camera is of such low quality that it does not allow the method to determine the covered user's age status, the outcome is inconclusive.

Where an age assurance method results in an inconclusive age assurance outcome, the covered operator should direct the covered user to re-attempt the age assurance method or undergo one or more alternative age assurance methods (where available) until a method leads to an age status determination for that covered user or until all available methods have been attempted in good faith with no determination reached. Defining inconclusive age assurance outcomes is key to how the proposed rule allows covered operators to offer a waterfall of age assurance methods, as described in Part III.D. In a waterfall, operators offer multiple age assurance methods that might be highly effective in certain conditions but unable to make a determination in others.

Under section 700.4(b), every age assurance method used by a covered operator must meet the accuracy minimum and at least one method must meet the total accuracy minimum. Inconclusive age assurance outcomes are not included in the calculation of the accuracy minimum—the accuracy minimum is determined by dividing the number of false positives by the number of age status determinations. The individuals with inconclusive outcomes simply are not considered. This is because with an inconclusive outcome, the covered operator is not wrongly designating a minor user to be an adult. Instead, such a user falls in a separate category—an individual for whom the operator was not able to determine age status one way or another and to whom the covered operator can provide another age assurance method. An inconclusive outcome is, thus, not the same as a false positive.

A covered operator may offer a covered user a method like email verification, which might have a significant number of inconclusive results but very few false positives, because it is a low friction method. Allowing a covered operator to offer methods that meet the required false positive rates without considering inconclusive outcomes gives covered operators the flexibility to use multiple methods that best suit their users' preferences and to consider the costs of different, effective age assurance methods.

However, inconclusive outcomes must be counted in the total accuracy minimum. Specifically, the total accuracy minimum is equal to: (number of false positives + number of inconclusive outcomes)/all users completing age assurance methods. To ensure every user of a

platform is able to use a method that can make an age status determination and meets accuracy minimum (including some who receive inconclusive results from certain methods), a covered operator must have at least one age assurance method that does not exceed the maximum false positive rates inclusive of instances in which the age assurance method cannot render a result regarding the covered user's age status. Put another way, this requirement ensures that at least one age assurance method offered by a covered operator can be successfully completed by virtually all users while allowing covered operators to adopt a waterfall of methods.

21. Information Persistently Associated

The proposed rule defines "information persistently associated" as any information that the covered operator associates with the user or the user's device over time. The proposed definition also states that information is not persistently associated if the covered operator does not use the information to recognize the user or the user's device over time. The OAG seeks comments on the proposed definition of information persistently associated.

The proposed rule defines this term to assist operators in determining what is and is not an addictive feed as defined in section 700.1(c)(2), which implements G.B.L. § 1500.1(A). Central to this definition is that information persistently associated means information the covered operator associates with the user over time. The term does not include information about the user simply because the information remains the same and is associated with the user over time more generally. Instead, recommending, selecting, or prioritizing media based on information associated with a user or device for a one-time purpose without retaining that information to recognize the user or device later is not information persistently associated for purposes of the proposed rule. For example, if an operator uses information such as a device ID for a one-time purpose such as to carry out delivery of media to a specific device and does not retain that device ID for further processing, then the operator is not using the device ID as information persistently associated with the user or the user's device. As another example, an operator may process a device ID in order to identify when the user has clicked on a webpage link for the purpose of changing the link color while the user remains on that webpage. Temporary use of the device ID for this purpose is not "information persistently associated" with the user or the user's device. However, if the operator continues to save and use the device ID for any purpose after the user has closed or otherwise exited the webpage, then the device ID has been "persistently associated" with the user or the user's device by the operator.

22. Media

The OAG proposes defining "media" as text, an image, or a video, consistent with G.B.L. § 1500(5).

23. Method Circumvention

The proposed rule defines "method circumvention" as submission of false data or interference with an age assurance method. It is assumed that method circumvention will be

employed most commonly by covered minors that wish to be treated as adults based on an incorrect determination of adult status by the age assurance method applied.

The types of method circumvention vary from simple to highly sophisticated and, in light of advances in AI-based technology, new forms can be expected to emerge on a regular basis. The annual certification requirement includes testing to determine whether the age assurance method meets the 98% method circumvention detection requirement that is part of the accuracy minimum and total accuracy minimum. Because annual testing may be insufficient to defeat emerging forms of method circumvention, however, covered operators also have an obligation to monitor reports and data regarding age assurance methods offered for signs of method circumvention and to address the detection of new or previously undetected forms of method circumvention in real time, under section 700.4(d)(3) of the proposed rule.

24. Minor

The proposed rule defines "minor" as an individual under the age of eighteen, consistent with G.B.L. § 1500.6.

25. Monthly Active User

The proposed rule defines "monthly active user" as a user who, in the previous calendar month or the one-month average measured across the previous calendar quarter, has accessed the online platform of an operator and remained on that platform for at least one minute. In proposing this defined term, OAG facilitates having a relevant metric for counting all users that intend to access one or more services offered by the covered operator's platform and to exclude incidental or inadvertent platform access or access for reasons other than to use the platform, including by bots or automated entities. The OAG seeks comments on the proposed definition of monthly active user.

While monthly active user is a metric commonly measured by software platforms, what constitutes a monthly active user is not consistently defined or measured across the industry. After studying a wide cross-section of user definitions across platforms, including daily and weekly as well as monthly active users, OAG proposes this definition of monthly active user with the intention of being as inclusive as or more inclusive than the majority of platforms when counting users.

The number of monthly active users is relevant to determine whether a covered operator qualifies as an exempt operator and to assist in defining addictive online platform. It is not necessary for platforms that track daily or weekly users, or track monthly users with a less inclusive formula than offered in this definition, to re-calculate monthly active users by this formula in order to claim exempt operator status, so long as they can later demonstrate that if they had used the monthly active user definition in calculating users, the outcome would have been the same.

26. Nighttime notifications

The proposed rule defines "nighttime notifications" as notifications concerning an addictive feed that are sent to a covered minor between the hours of 12 AM Eastern and 6 AM Eastern, consistent with G.B.L. § 1502. Notifications required by applicable federal, state, or local laws are not "nighttime notifications." The proposed rule seeks comment on the definition of nighttime notifications.

The OAG clarifies that some notifications during sleep hours may be required by law and that the rule does not apply to those notifications. Typically, a notification falling into this narrow exception will encourage the user to take action outside of the addictive online platform rather than stay on the addictive feed. Although OAG is not aware of any such requirements at this time, covered operators may be required to send notifications by emergency order under the law in certain exceptional cases.

Finally, OAG notes that to be a nighttime notification, the notification must be concerning the addictive feed. For example, a notification from a covered operator during the hours outlined in the statute that directs a user to resources outside of the addictive feed, such as an emergency alert center that is separately hosted and can be accessed without entering the addictive feed, is not a nighttime notification.

27. Online Platform

To streamline multiple provisions of the proposed rule, OAG defines "online platform" as a website, online service, online application, or mobile application. The Act uses the phrase website, online service, online application, or mobile application throughout. OAG uses the term online platform in recognition of current technology. Platforms connected to the Internet may be accessed in multiple ways through various and diverse types of devices, but any of these platforms may have design features meeting the definition of an addictive feed or a nighttime notification.

28. Parent

The OAG proposes defining "parent" as an individual who is recognized under New York State law as: (1) acting in parental relation to the covered minor; (2) having the status of a legal guardian or custodian for the covered minor; or (3) in the case of an individual who otherwise would qualify as a minor, having the status of a parent to the covered minor. The OAG seeks comment on the proposed definition of parent.

This definition is consistent with both G.B.L. § 1500.8, which defines parent as "parent or legal guardian," and with existing New York State law, which further defines parent in recognizing the rights of individuals to oversee their children's upbringing in an array of

contexts.[60] For example, Education Law § 2-d, which governs the rights of parents regarding the use of their children's data in education, defines a "parent" as "parent, legal guardian, or person in parental relation to a student."[61] New York family law similarly recognizes that an individual may have the status of a parent by birth, by adoption, or by virtue of being "in parental relation" to the child.[62] "In parental relation" also appears in laws such as Public Health Law § 2504 governing the rights of parents regarding the provision of healthcare services to their children. This term has well-settled meaning in these areas.[63] As with children's healthcare, education, and family law, the Act recognizes the importance of parental oversight in supporting safe and healthy childhoods, so relying on existing New York State law in these areas to define the term parent is consistent with its objectives.

The proposed definition also recognizes that a minor may have more than one individual who acts "in parental relation" to the minor, and in such a case, each individual may have the right to grant consent on behalf of that minor. This approach is also consistent with federal laws such as the Family Educational Rights and Privacy Act of 1976 (FERPA).[64]

Finally, existing New York State law recognizes that in cases where an individual who is under the age of eighteen also has the status of a parent (by birth or marriage) to a child, that individual is capable of overseeing their child's upbringing. For example, under Pub. Health Law § 2504(2), such individuals may grant consent for the provision of healthcare services to their child. Consistent with these laws and in these limited circumstances, the proposed rule would allow such individuals to be recognized as parents for purposes of the Act.

---

[60] This approach also is consistent with federal laws such as the Family Educational Rights and Privacy Act. *See* 34 C.F.R. § 99.3 (defining parent to include "a natural parent, a guardian, or an individual acting as a parent in the absence of a parent or a guardian").

[61] Educ. L. § 2-d(1)(h).

[62] Comp. Codes R. & Regs. tit. 10, § 69-4.1(ai).

[63] *See, e.g.* Educ. L. § 2(10) (defining "in parental relation" as "parents, guardians or other persons, whether one or more, lawfully having the care, custody or control of such child, including persons who have been designated pursuant to title fifteen-A of article five of the general obligations law as persons in parental relation to the child").

[64] 34 C.F.R. § 99.3 (definition of "parent") and 34 C.F.R. § 99.4 ("An educational agency or institution shall give full rights under the Act to either parent, unless the agency or institution has been provided with evidence that there is a court order, State statute, or legally binding document relating to such matters as divorce, separation, or custody that specifically revokes these rights").

29. Person

The proposed rule defines "person" to include individuals as well as partnerships, corporations, associations, or any other form of business enterprise.

30. Self-Declaration

The proposed rule defines "self-declaration" as an action by a covered user to indicate that user's age or age status. This can include a written representation by the covered user or an affirmative, recordable action such as clicking a confirmation button.

After reviewing numerous studies documenting the accuracy of self-declaration, OAG concludes that historically, self-declaration as an adult has not yielded results accurate enough to meet the accuracy minimum and no age assurance method exists today that would enable self-declaration without additional information or analysis to meet the accuracy minimum. As such, self-declaration as an adult is not an acceptable method to confirm adult status under the proposed rule.

Conversely, proposed section 700.4(a)(1) states self-declaration as a minor constitutes actual knowledge by an operator of a covered user's minor status. This provision assumes that, specifically for purposes of determining access to an addictive feed, an age assurance process is unlikely to yield false self-declarations of minor status. Allowing self-declaration as a minor therefore reduces the burden on both covered operators and covered minors to utilize additional age assurance methods for users self-declaring as minors. This provision does not, however, prevent covered operators from conducting age assurance methods for reasons unrelated to compliance with the proposed rule, including to ensure compliance with other legal obligations or with the covered operator's trust and safety guidelines.

31. Technical Information Concerning a User's Device

The proposed rule defines "technical information concerning a user's device" as information that is associated with the user's device and technical in nature. Technical information concerning a user device: (i) is not information linked to the user's identity; (ii) cannot include information linked, directly or indirectly, to the user's previous interactions with media generated or shared by other users; and (iii) is not otherwise processed for the purpose of providing an addictive feed or nighttime notifications. An online platform cannot evade the Act and proposed rule by arguing the use of information associated with the user's device is technical information concerning the user's device to present that user with an addictive feed. The OAG seeks comments on the proposed definition of technical information concerning a user's device.

Technical information concerning a user's device includes the kind of user information necessary to be able to deliver the online platform to a user from a technical perspective. For example, a device's language setting would be technical in nature. In the proposed definition of

addictive feed, this term is used to describe one of the conditions under which use of information associated with a user does not render an online platform an addictive feed. Thus, an operator's use of the language setting to filter out content in other languages would not violate the proposed rule.

As another example, if a user chooses to enable closed captions while watching videos, the operator may use the user's device ID for the purpose of automatically enabling closed captions on those videos, provided that the operator does not link that device ID to the user's identity or to any other information about the user's previous interactions with media generated or shared by other users, and the operator does not otherwise process the device ID for the purpose of providing an addictive feed or nighttime notifications. Similarly, the operator may determine that the user's device is using a specific operating system in order to provide a version of its online platform that is optimized for that operating system. In doing so, the operator may not link the operating system information to the user's identity or to any other information about the user's previous interactions with media generated or shared by other users, and the operator may not process the operating system information for the purpose of providing an addictive feed or nighttime notifications. If the operator fails to comply with all of these requirements, the operator is not using the operating system information within the meaning of "technical information concerning a user's device."

A final example is when an operator translates the IP address associated with a user or a user's device into an estimate of the user's general location. If the operator then uses the location information to apply the same rules or policies to that user as it does to any other users in that location (for example, to comply with a state law like the Act, or to block content that the operator is not licensed to make available in the State of New York), the operator may consider the location information to be "technical information concerning a user's device." However, the operator must carefully consider whether the location information may be so specific as to be "linked" to the user's identity. It also cannot use the location information to provide an addictive feed or nighttime notifications.

32. Total Accuracy Minimum

The proposed rule defines "total accuracy minimum" to mean a combined rate of false positives and inconclusive age assurance outcomes for an age assurance method that is equal to or less than 0.1% of minors aged 0 to 7; 1% of minors aged 8 to 13; 2% of minors aged 14 to 15; 8% of minors aged 16; 15% of minors aged 17, along with a 98% rate of detection of method circumvention. The OAG seeks comments on the proposed definition of total accuracy minimum.

As described in the section addressing inconclusive age assurance outcomes, the total accuracy minimum differs from the accuracy minimum in that the rates include inconclusive age assurance outcomes as well as false positives, whereas the accuracy minimum includes only false positives. This distinction recognizes that some age assurance methods may yield low false

positive rates and so may positively impact a covered operator's ability to administer age assurance methods, particularly where the method minimizes user friction. At the same time, to ensure that the highest number of covered users can receive a determination as to age status, at least one method offered by a covered operator must render minimal inconclusive outcomes as well as false positive rates.

33. User

The proposed rule defines "user" as a person or entity that uses a covered operator's online platform or any portion thereof and is not acting as the covered operator or an agent or affiliate of the covered operator, consistent with G.B.L. § 1500.4. Consistent with the definition of covered user, this definition excludes any account on the operator's online platform or any portion thereof that belongs to the operator or to the operator's agents or affiliates. Although the Act does not define user, OAG proposes defining the term user for clarity. The rule does not apply to users who are not covered users. However, in setting certain standards, such as determining whether an online platform is an addictive online platform, the platform's operation as a whole, as opposed to with respect to users only in the State of New York, is relevant.

34. Valid Consent

The proposed rule defines "valid consent" as consent that is clear and unambiguous, specific, informed, and freely granted. The OAG seeks comments on the proposed definition of valid consent, including the definitions of terms used within the definition.

This proposed definition incorporates principles to address the challenges of understanding an individual's intent and capacity to signal when a decision has been made and what that decision is in the online/digital environment. The proposed definition also reflects consideration of laws in other states as well as online/digital contracting principles across multiple jurisdictions. The proposed definition thus requires a covered operator to account for the differences between obtaining consent from an adult parent or legal guardian and from a covered minor.

Valid consent under the proposed definition does not include any circumstance in which the operator obtained the consent via a method that has the purpose or substantial effect of obscuring, subverting, or impairing an individual's decision-making.[65] These are sometimes referred to as "dark patterns" and such methods are incompatible with an individual's ability to provide valid consent. For example, a covered operator may not state during the consent process that the individual will have a "poorer" or "less enjoyable" experience on the online

[65] *See* Fed. Trade Comm'n, *Staff Report: Bringing Dark Patterns to Light* 14-16, 18 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

platform if they do not grant consent. As another example, a covered operator may not repeatedly prompt an individual to grant consent after they have refused to do so. A covered operator also may not require an individual to discuss their decision prior to providing the option to make a choice, such as by interacting with the covered operator's customer service representative or a chatbot or filling out survey questions.

The proposed rule also defines the terms "clear and unambiguous," "specific," "informed," and "freely granted" to provide additional guidance as to these foundational principles of valid consent.

"Clear and unambiguous" means an expression of consent through an individual's affirmative action. An individual must take an affirmative action directly related to the request for consent in order to signal their grant of valid consent. Fleeting, unconscious, or unintentional interactions with an online platform are insufficient to constitute valid consent. Interactions unrelated to the request for consent are also not sufficient to signal valid consent. For example, it is not valid consent if the individual simply closes a window, scrolls past a notice, or clicks on another part of the screen outside of the notice.

"Specific" means (1) the request for consent is presented separately from any other request by the covered operator and (2) consent must be separate for an addictive feed or for nighttime notifications. A covered operator may request consent for an addictive feed and for nighttime notifications in a single transaction, provided that consent may be granted separately for each feature. An individual should never be presented with only the option to grant consent to both features or refuse consent for both features.

Covered operators must present requests for consent under the Act separately from other requests, such as requests to enable or disable other features, requests to sign up for emails or notifications, or requests to agree to terms of service. Requiring an individual to grant consent under the Act as part of agreeing to an online platform's terms of service, or as part of agreeing to access another feature on the online platform, is not valid consent. A covered operator may, however, include a request for consent in an account creation workflow that includes other notices to the user provided the request for consent is presented in a separate, distinct manner and the user's decision to grant or refuse consent at that stage does not trigger discriminatory conditions in violation of G.B.L. § 1504 of the Act. As further discussed in Part III.B and C , addressing parental consent, a covered operator also may include a request for consent under the Act in the same transaction as a request for consent under the Children's Online Privacy Protection Act ("COPPA"), provided that the respective notices required under the Act and under COPPA are separately presented.

"Informed" means a notice that is provided in plain language and is understandable and accessible to the target audience. Any such notice must be provided in at least the twelve most commonly spoken languages in the State of New York consistent with N.Y. Executive Law § 202-a

and G.B.L. § 1506 and may be provided in written or any other form that otherwise complies with these regulations. For example, this may include an audio recording of the notice.

An individual must be presented with a notice explaining to them, in simple, clear terms that can be understood without any special education or training, what they are consenting to. Since the rule contemplates that consent will be requested from both covered minors and their parents, the notice must also take into consideration these different audiences. A covered minor may not be as able as a parent to read or understand complex sentence structure or uncommon words and may not have the attention span to follow dense blocks of text. It may also be harder for a covered minor than a parent to navigate certain design features, such as dropdown menus or toggles. When a notice is presented to a covered minor, additional effort should be made to ensure that notice is appropriately tailored to its audience and avoids potentially misleading or deceptive language or design elements. This plain language approach, requiring that any notice take into account whether the audience for a notice is a parent or a minor, is also consistent with the general approach of the Federal Trade Commission ("FTC") regarding how to communicate with minors.[66]

To avoid unfairly disenfranchising certain parents and covered minors and to remain consistent with state and federal disability laws, a notice must also be accessible to those who may otherwise have challenges to understanding text-only notices, such as individuals with visual impairments, who are illiterate, or who have physical or other impairments to using devices that allow access to online platforms. To give covered operators maximum flexibility in addressing accessibility concerns, the notice may be presented in any form that satisfies the requirements set forth in the rule. For example, a covered operator may determine that a significant portion of parents will benefit from being provided with a video version of the notice, including video instructions on how the parent can register their consent choice. A covered operator is not required to provide a video version of the notice.

"Freely granted" means the process for refusing consent is at least as easy to use as the process for granting consent in any request for consent. Additionally, a covered operator must allow previously granted consent to be easily modified or withdrawn at any time. For example, the covered operator cannot make the option to grant consent more prominent or visible than the option to refuse consent or force the individual to navigate away from the option to grant consent in order to find the option to refuse consent. The covered operator also cannot make it difficult for the individual to change their choices later, such as by requiring the individual to submit a customer service request by phone, email, or online chat when the individual initially granted consent via a simple online process that did not require customer service assistance.

---

[66] Fed. Trade Comm'n, *.com Disclosures: How to Make Effective Disclosures in Digital Advertising* 11 2013), https://www.ftc.gov/system/files/documents/plain-language/bus41-dot-com-disclosures-information-about-online-advertising.pdf; Fed. Trade Comm'n, *Staff Report: Bringing Dark Patterns to Light*, n.65 *supra*, at 18.

35. Zero-Knowledge Proof Age Assurance

The proposed rule defines "zero-knowledge proof age assurance" as an age assurance method that allows a covered user to accurately verify their age status in a privacy-preserving manner. The OAG seeks comments on the proposed definition of zero-knowledge proof age assurance.

Zero-knowledge proof age assurance allows a covered user to transmit proof of age status to the covered operator without sharing additional personal information, such as the contents of government-issued identification. The technology utilizes a third-party facilitator, such as a digital wallet or app, to verify a user's age or age status. That verified status can be stored with the facilitator or on the user's device and can be communicated to the covered operator upon request. If the third-party facilitator sends confirmation of the covered user's age or age status to the covered operator, it does so without knowing the covered operator's identity. This method is sometimes referred to as a "double blind" age assurance method because no one other than the user is aware of both the user's personal information and the identity of the operator requesting that information. The method can constitute an effective age assurance method that maximizes user privacy and data security.

The covered operator is responsible for ensuring that the technology and signals underpinning zero-knowledge proof age assurance are sufficient to transmit proof of covered user age status that meets the accuracy minimum. Because zero-knowledge proof age assurance methods are new but increasingly available technology, allowing such methods will provide additional options for covered operators to utilize effective age assurance methods that also protect the interests of covered users.

B. Section 700.2 Prohibition of addictive feed

1. Default and exceptions

In section 700.2(a), OAG proposes a default prohibition of addictive feeds from covered operators to covered users. The section also proposes two exceptions to the prohibition, both of which are the obligation of the covered operator to effect: either the covered operator must establish the covered user's adult status through an age assurance method consistent with the requirements of 700.4 or, if the covered user is determined to be a minor (through actual knowledge as defined in section 700.4(a)), the covered operator must obtain verifiable parental consent that complies with the obligations in 700.2(e).

Proposed section 700.2(b) makes clear that covered operators are not required to offer a method of parental consent to covered minors. Under this proposed framework, should a covered operator elect not to make a method of parental consent available, section 700.2(a)(2) would not be available to that covered operator as an exception to the default prohibition of

addictive feeds and the covered operator would not be able to provide an addictive feed to any covered minor.

2. Exempt online platforms

Section 700.2(c) excludes "exempt online platforms," which under the proposed definition in section 700.1(q), means online platforms with fewer than 5 million monthly active users or fewer than 20,000 monthly active users who are covered minors, measured in accordance with that proposed definition. Covered operators whose total monthly active users do not reach one of these thresholds are not required to comply with the proposed rule until such time as a threshold is reached or exceeded, so long as the applicable platform's primary users are not minors.

As described in greater detail in Part IV, although the cost of implementing age assurance methods as a portion of all costs remains relatively low even for platforms below the threshold, the percentage of revenue required to support age assurance methods grows for implementation and for annual maintenance. Beyond these costs, however, OAG's analysis of available market data demonstrates that platforms with addictive feeds typically monetize user engagement through advertising sales, which generally does not bring in material revenue until the platform's global monthly active users exceed 5 million. Covered operators in an early stage of the economic cycle instead focus on establishing and growing the platform's user base and demonstrating the viability of its business model. Requiring early-stage platforms to take on age assurance methods could ultimately inhibit competition and market entry by diverting resources and focus, thereby offering an advantage to the entrenched players in the market, which were able to grow and mature their businesses without these obligations. Platforms at this stage also may lack internal resources to manage a project like age assurance method implementation and the related compliance obligations, which could potentially lead to adverse outcomes for users.

While allowing platforms with fewer than 5 million monthly active users to defer compliance with the proposed rule will result in some covered minors continuing to receive addictive feeds, the negative impact of this exemption is limited, for a few reasons. First, under the proposed rule, covered operators whose primary users are minors are not eligible for this exemption; compliance is necessary regardless of company size to protect their intended audience of minor users. Second, as soon as a covered operator reaches the 5 million-user threshold, it must comply with all aspects of the proposed rule within 180 days. Companies approaching the 5million-user limit, or even with the future intent of doing so, are on notice and must prepare for compliance and tailor their business model accordingly.

The exception for platforms with fewer than 20,000 covered minor users accounts in part for the Legislature's mandate that OAG consider the "audience" of the online platform in G.B.L. § 1501(2)(b). Online platforms with fewer than 20,000 covered minors who are monthly

active users of the platform are exempt. This proposed exception also allows covered operators to avoid the costs of compliance and accounts for the possibility that this cost may not be commercially reasonable when compared to the modest benefit to the covered operator of maintaining a relatively small number of users in the State of New York. Allowing exemption from compliance on this basis incentivizes operators to offer services to users in the State of New York, including covered minors, without bearing the costs of age assurance methods that complies with the proposed rule until such time as doing so becomes commercially reasonable.

The OAG considered but ultimately does not propose a number of other thresholds for an exemption. For example, a threshold based on annual revenue raised feasibility concerns because platforms could be earning insubstantial or no revenue, and in some instances might adopt a non-revenue-maximizing business model, but nonetheless could be subjecting large numbers of minor users to harm from addictive feeds. Additionally, an exemption based upon the amount of time users spend on the platform was considered but this metric raised potential concerns regarding measurement and related enforcement. Finally, requests from stakeholders to limit application of the proposed rule to only platforms perceived as particularly harmful to minors (for example, exempting news or educational sites, or platforms primarily directed to an older audience like a professional networking site) were rejected as is inconsistent with the statutory language and purpose of protecting minors from addictive feeds as a design feature, which cuts across all subject matter and content. Any platform that exceeds 5 million monthly active users or 20,000 monthly active users who are minors and that offers an addictive feed to minors, regardless of the content or purpose of the platform, must comply.

3. Identifying covered users

The covered operator is obligated to determine whether each of its users is a covered user, which necessitates understanding whether the user is located within the State of New York. The OAG is aware that many platforms already have data regarding the geographic location of users and use that data for various purposes including marketing or other commercialization of the user's engagement, or selection of personalized content for the user. Under the proposed rule, covered operators must take this data into account, to the extent it is reliable. This data also may include technical information concerning a user's device, as defined in section 700.1(ff), which is presumed to include the IP address of the user's device. Covered operators may use the same decision-making process already in place for commercial or content-related uses of user location data to determine whether a user is a covered user for purposes of compliance with the proposed rule.

Some users may attempt to conceal or misrepresent their location to avoid application of the Act. The proposed rule obligates the covered operator to take reasonable steps to investigate and detect such attempts, and in the event they are detected, to determine whether the user is a covered user by employing reasonable methods utilizing available data.

4. Parental consent requirements

a. Background

i. General consent management systems

Collecting consent from users of an online platform is both a widespread regulatory concept and common technology. Many jurisdictions impose some kind of legal requirement to collect valid consent from a user in an online environment in order to process their data (or collect the individual's refusal to grant consent for the data processing), maintain a record of that consent, and allow the individual to later update their consent choices.[67]

In response to these laws, platform technology allowing users to record and manage their consent choices rapidly developed and continues to evolve. This technology, commonly known as a consent management system, became widespread after the EU's General Data Protection Regulation ("GDPR") came into effect in May 2018, and has since grown into a thriving and sophisticated privacy technology industry. Current offerings in the marketplace include the ability to set up consent management interfaces tailored to the requirements of multiple jurisdictions, with some allowing an operator to display different interfaces (including different languages) to users in different jurisdictions.

Consent management systems vendors often offer modular services, where an operator may choose to have the vendor manage the entire user interface, or may have the vendor operate only certain parts while internally handling the rest.[68] For example, an operator may decide to have the vendor provide the user interface that collects a user's initial consent choices but handles the actual processing of the user's choice internally. Current consent management systems thus give operators great flexibility in deciding how to particularize a consent system to best suit their online platform, considering factors such as costs, resources, user experience, and ease of ongoing maintenance.

General consent management systems already address issues such as accuracy, reliability, security, and commercial feasibility concerns, which are all concerns a parental

---

[67] The first U.S. jurisdiction to impose a general requirement to give users the ability to refuse consent to online data processing was California in 2020 with the California Consumer Privacy Act. 1.81.5 Cal. Civ. § 1798.120. As of July 2025, thirteen states have comprehensive privacy laws in effect that have such a requirement. Int'l Ass'n of Priv. Pros., *U.S. State Privacy Legislation Tracker 2025,* https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf (July 7, 2025). Another five states have passed laws with such requirements that go into effect within the next year. *Id.*

[68] *See, e.g.,* Digital Advertising Alliance, *Coalition of Privacy Self-Reg Orgs Launch Uniform Approach to CMP-Specific Controls and Network-Wide Privacy Choices*, Feb. 14, 2023, https://digitaladvertisingalliance.org/press-release/coalition-privacy-self-reg-orgs-launch-uniform-approach-cmp-specific-controls-and.

consent system must also tackle. A general system must be able to uniquely identify a user's consent record so it may be stored, retrieved, and modified as necessary. The system must also comply with information security requirements imposed by various laws, since the consent record itself generally contains personal data governed by these laws. Since these systems were developed in response to general-purpose privacy laws, their customers include nearly every type of online business, small and large. A system to collect parental consent is a particularized version of a general consent management system—versions of which, of course, are used today.

ii. COPPA and parental consent methods

Parental consent management systems were adopted early in the internet age. In 1998, Congress passed COPPA, mandating parental consent before personal information can be collected from a child under 13.

The FTC first issued regulations implementing COPPA in 1999 (the "COPPA Rule"), including its requirements for obtaining "verifiable parental consent," and has periodically updated these regulations.[69] Under all versions of the COPPA Rule, methods of collecting verifiable parental consent must be "reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent."[70]

The COPPA Rule currently recognizes eight satisfactory methods of parental consent, the last two of which were added in the 2025 amendment of the COPPA Rule[71]:

1. consent form signed by the parent;
2. authenticated credit card or debit card transaction;
3. toll-free telephone call;

---

[69] 16 C.F.R. § 312 (2025). *See also* Fed. Trade Comm'n, *Children's Online Privacy Protection Rule, Federal Register Notices*, https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa (last accessed July 28, 2025).

[70] *Compare* Children's Online Privacy Protection Rule, 64 Fed. Reg. 80, 22750, 22756 (Apr. 27, 1999) (to be codified at 16 C.F.R. § 312) (proposing first version of 16 C.F.R. § 312.5(b) *with* COPPA Rule, 90 Fed. Reg. 16918, 16980 (Apr. 22, 2025) (to be codified at 16 C.F.R. § 312) (publishing latest final version of same provision).

[71] 16 C.F.R. § 312.5(b). The COPPA Rule outlines two options for verifying government-issued identification, by comparing to an appropriate database, 16 C.F.R. § 312.5(b)(2)(v), and by using facial recognition technology to check against the individual's appearance, provided a human reviewer is also utilized, 16 C.F.R. § 312.5(b)(2)(vii). Although the facial recognition option was only added in the 2025 COPPA rulemaking, COPPA Rule, 90 Fed. Reg. at 16952, a method for using government-issued identification has been present since the 2013 version of the COPPA Rule, 12 Fed. Reg. 3972, 3987 (Jan. 17, 2013) (to be codified at 16 C.F.R. § 312).

4. video conference;

5. check of government-issued identification belonging to the parent;

6. email paired with an additional confirmatory step;

7. knowledge-based authentication consisting of a series of questions where the answers are unlikely to be correctly guessed, or to involve information easily known to the child; and

8. text message paired with an additional confirmatory step;

Operators governed by COPPA are not limited to these methods and may use others that satisfy the requirements for verifiable parental consent.[72]

As evidenced by the recent addition of new satisfactory methods for verifiable parental consent, technical innovation in methods for seeking parental consent continues.[73] Many companies have been able to integrate COPPA-compliant methods of verifiable parental consent while continuing to operate products and services "directed to children" under COPPA.[74] This federal framework for verifiable parental consent, which has evolved to account for changes in regulatory requirements, business needs and technology, has laid the groundwork for companies to develop further technical methods of obtaining parental consent, including the process the proposed rule outlines.

---

[72] The COPPA Rule also provides for two mechanisms to review new methods of parental consent, one where review is undertaken by the FTC itself, 16 C.F.R. § 312.12(a), and one where review is undertaken by third-party safe harbor programs certified by the FTC, 16 C.F.R. § 312.5(3)(b). Both mechanisms have been processing submissions for well over a decade.

[73] As discussed *infra* in Part III.D, the 2025 age assurance trial commissioned by the Australian government in preparation for implementation of mandatory age assurance by social media platforms assessed numerous age assurance providers including 12 providers offering a variety of parental-consent methods and found that seven had technology readiness levels of 7-9, which denotes product availability ranging from an operational beta/pilot (level 7) to an operational commercially deployable product (level 9). Age Check Certification Scheme, *Age Assurance Technology Trial Final Report: Part H – Parental Consent* at 44, September 1, 2025, https://www.infrastructure.gov.au/sites/default/files/documents/aatt_part_h_digital.pdf.

[74] The FTC has estimated as part of the 2025 COPPA Rule that over 6,000 current operators are subject to COPPA, with an additional 430 new operators expected to enter the market every year. COPPA Rule, 90 Fed. Reg. at 16972. This is a significant increase over its estimate in the 2013 COPPA Rule, which estimated 2.910 current operators and 280 new operators expected to enter the market every year, COPPA Rule, 78 Fed. Reg. at 4002, strongly indicating that new operators have not been deterred by the need to comply with COPPA.

b. Verifiable parental consent requirements

The proposed rule implements G.B.L. § 1501(4), requiring OAG to promulgate rules "identifying methods of obtaining verifiable parental consent" to provide an addictive feed. Covered operators are not required to provide users with a method to obtain verifiable parental consent. For those covered operators that choose to provide minors with the option of seeking parental consent to access an addictive feed, the proposed rule requires a covered operator to implement a two-step process. In the first step, section 700.2(e)(1), the covered operator (i) must notify the covered minor that the covered operator cannot provide access to an addictive feed under New York law without obtaining verifiable parental consent and (ii) must provide the covered minor with the option to have the covered operator request verifiable parental consent on their behalf.

The covered operator must obtain valid consent from the covered minor to send the request for verifiable parental consent. Without the covered minor's request and consent, the covered operator cannot send a request or otherwise contact the covered minor's parent to obtain consent. Not all covered minors may wish to access an addictive feed or to request consent from their parents to do so. Consistent with the intent of the Act to limit the harmful effects of addictive feeds on minors, if a covered minor does not seek access to an addictive feed, a covered operator cannot contact the parent.

In the second step, section 700.2(e)(2), provided the covered minor provides valid consent, the covered operator (i) must provide the parent with notice that the covered operator cannot provide the covered minor with access to an addictive feed under New York law without obtaining verifiable parental consent and (ii) must provide the parent with access to a method of verifiable parental consent meeting the proposed rule's requirements. This is consistent with generally accepted principles of valid consent, which require notice as well as a mechanism for collecting consent. The proposed rule specifies the requirements for notice in section 700.2(e)(4) and for collecting consent in section 700.2(e)(5), including the proposed rule's interaction with COPPA in section 700.2(e)(6), as described later in this section.

The proposed rule requires a covered operator to provide an easy to use, accessible method by which a covered minor or their parent can withdraw their consent at any time, consistent with the proposed definition of valid consent, in section 700.2(e)(2). In addition, a covered operator may not require a covered minor or a parent to interact with a live representative in order to withdraw their consent, unless interacting with a live representative was the method by which they initially granted consent. Withdrawing consent should not be more burdensome than granting consent and forcing an individual to first speak to a live

representative is likely to discourage the user from exercising the right to withdraw consent or dissuade them from doing so.[75]

Proposed section 700.2(e)(3) prohibits the covered operator from renewing a request for verifiable parental consent once a parent has refused to grant consent, unless the covered minor requests that the covered operator send a renewed request. Consistent with G.B.L. § 1503, this prohibition protects the privacy of the covered minor by ensuring that the covered operator is not communicating with the parent about the addictive feed or nighttime notifications without the covered minor's knowledge and consent. It also protects the parent's privacy by ensuring the covered operator does not repeatedly send unneeded communications. Moreover, nagging an individual with similar communications is commonly recognized as a potential misleading or deceptive practice that undermines the individual's ability to grant valid consent.[76]

The OAG notes that a minor may request parental consent from a parent and a parent may give consent regardless of the parent's physical location or legal residence.[77] This is consistent with the proposed definition of "parent" and with existing definitions of "parent" under existing New York State law, which do not treat out-of-state parents of a minor resident in the State of New York differently from in-state parents.[78]

i. Parental consent notice requirements

Proposed section 700.2(e)(4) specifies requirements to ensure operators provide clear and conspicuous notice before any request for verifiable parental consent, consistent with general principles for online disclosures and informed consent.[79] The proposed notice must include three components: (i) identification of the addictive online platform and (ii) the covered

---

[75] The proposed rule does not prohibit covered operators from providing access to live customer support, generally.

[76] Fed. Trade Comm'n, *Staff Report: Bringing Dark Patterns to Light*, n.65 *supra*, at 24-25. This applies equally to a minor or their parent. A covered operator will not be deemed to have obtained valid consent from either if it was obtained via nagging them after they initially refused to grant it.

[77] The geographical limitation in G.B.L. § 1507(1) applies to the location of the user and does not apply to parents or limit parental rights under the Act.

[78] *See, e.g.*, Educ. L. § 2(10).

[79] Fed. Trade Comm'n, *.com Disclosures: How to Make Effective Disclosures in Digital Advertising* 11 2013), https://www.ftc.gov/system/files/documents/plain-language/bus41-dot-com-disclosures-information-about-online-advertising.pdf; Fed. Trade Comm'n, *Staff Report: Bringing Dark Patterns to Light*, n.65 *supra*, at 18; see Wu v. Uber Techs., Inc., 43 N.Y.3d 288, 302 (N.Y. 2024) (inquiry notice requirement for online contract formation).

minor's account, profile, or username (as applicable) as well as (iii) information about the nature of the consent being sought.

The online platform should be identified because a covered operator may operate more than one online platform with an addictive feed. The specific account, profile, or username should be identified as a covered minor may have more than one on any given platform. The covered minor should be able to seek consent only for a specific account, profile, or username and should not be forced to request verifiable parental consent for all accounts.[80] Moreover, the notice should only identify the account, profile, or username for which the request is being sent, and should not include any other accounts, profiles, or usernames used by the covered minor, consistent with G.B.L. § 1503 clarifying that the Act does not require operators to provide parents with additional special access or control over the data of their minor.

Proposed section 700.2(e)(4)(iii) describes mandatory information the notice must state with equal prominence and in plain language that is understandable and accessible to the target audience. First, the provision proposes the disclosure inform the covered minor and parent that the law of the State of New York does not allow the covered operator to provide media to a minor using a feature in which the covered operator recommends, selects, or prioritizes the media based on information associated with that minor or that minor's device without parental consent, except in limited circumstances.

Second, the provision proposes the disclosure inform the covered minor or parent that a covered minor can access the online platform with a feed that does not include the prohibited feature, including while a request for verifiable parental consent is pending. Under G.B.L. § 1504, a covered operator cannot withhold access to their online platform simply because an individual is a minor or does not request or obtain parental consent to get an addictive feed. The disclosure ensures the covered operator does not imply the covered minor cannot use the online platform at all without parental consent. Finally, the provision proposes a disclosure that the covered minor or parent can modify or withdraw their consent, consistent with the proposed definition of valid consent.

ii. Parental consent methods

Proposed section 700.2(e)(5) specifies the requirements for any method for seeking verifiable parental consent. First, the covered operator must use an age assurance method to determine the parent's age status pursuant to section 700.4. As the same considerations will arise in determining a parent's age status and any covered user's age status, and to streamline and facilitate compliance, the requirements for administering age assurance methods for

[80] Similarly, a parent should not have to grant consent for all of their minor's accounts, profiles, or usernames and should be able to consider each separately.

parents are the same as for covered users. Consistent with G.B.L. § 1506(1), any instructions to the parent related to the determination of age status must be provided in at least the 12 most commonly spoken languages in the State of New York (determined pursuant to New York Executive Law § 202), in any form that otherwise complies with these regulations, including audiovisual form. Second, pursuant to proposed 700.2(e)(5), the method must provide an option to the parent to grant valid consent, consistent with the requirements outlined in the proposed rule's definition of valid consent.

As set forth in proposed section 700.2(e)(6)(iii), the method must also be reasonably calculated, in light of available technology, to ensure that the individual providing consent is a parent of the covered minor. This standard mirrors the parental consent requirement in the COPPA Rule. The standard allows a covered operator flexibility in choosing and tailoring a method to its specific online platform, while ensuring advancements in technology are not overlooked or discouraged by listing specific methods that may quickly become out of date.

Consistent with G.B.L. §§ 1501(5) and 1505, the proposed rule includes provisions requiring the method to include reasonable efforts to protect covered users' and parents' privacy and safety and to be reasonably calculated, in light of available technology, to account for the likelihood of circumvention, fraud, or misuse of the method. Requiring the parent to undergo age assurance may assist the operator's efforts to account for circumvention, fraud, or misuse of the method, but age assurance does not by itself satisfy this obligation.

A covered operator must consider how a covered minor, a parent, or an unrelated third-party may circumvent, commit fraud, or misuse a method of verifiable parental consent and take mitigating steps when implementing parental consent methods to protect both covered minors and their parents from privacy, security, and other harms.

Proposed section 700.2(e)(5)(vi) requires the method to include at least one option that does not require the parent to furnish government-provided identification, unless the covered operator collects or possesses a parent's government-provided identification to comply with other laws. This is consistent with the approach outlined in Section 700.4, as the same considerations apply.

Finally, proposed Section 700.2(e)(5)(vii) requires the method to include at least one option that does not require the parent to create an account with the covered operator or require the parent to purchase additional goods or services from the covered operator. Existing methods of verifiable parental consent approved by the FTC for use under [81] OBJ Both approaches

[81] Requiring a parent to grant consent separately on different devices also does not seem technically required. *See id.* (noting a parent can be asked to consent via being sent a one-time link and an authentication key

impose significant additional burdens on the parent that are not technically necessary and that may also result in unnecessarily withholding or degrading services to covered minors seeking consent, in violation of G.B.L. § 1504 and proposed section 700.9(b).

iii. Applicability of federal parental consent methods

Under proposed section 700.2(e)(6), if an addictive online platform is a "website or online service directed to children" as specified under COPPA and its implementing regulations or if a user is a covered minor under age 13, a covered operator may use the methods for verifiable parental consent approved by the FTC, provided that the covered operator incorporates three additional requirements from the proposed rule.

Proposed section 700.2(6)(ii) requires the covered operator to present a notice to the parent that complies with section 700.2(e)(4). This notice provides the parent necessary information on the subject of consent for access to an addictive feed. Allowing covered operators to provide only the COPPA-mandated notice, which generally covers collecting personal information from the minor, would not allow for valid consent under the proposed rule. However, and consistent with G.B.L. § 1507(2), the covered operator may, but is not required, to provide the notice required by this section and the COPPA notice in the same transaction, so long as the notices are presented separately. For example, a request for verifiable parental consent under COPPA can be completed via email to the parent that includes the COPPA notice. The same email may contain the separate notice required by this section.

Proposed section 700.2(e)(6)(iii) requires the covered operator to check that the method is reasonably calculated, in light of available technology, to account for the likelihood of circumvention, fraud, or misuse of the method. A covered operator must consider how a covered minor, a parent, or an unrelated third-party may circumvent, commit fraud, or misuse a method of verifiable parental consent and take mitigating steps when implementing the method. For example, a covered operator could easily monitor whether the same individual (as determined by an identifier such as an email address or an account with the covered operator's online platform) is purporting to be the parent of an unusually high number of minors. Previous FTC reviews of potential methods of verifiable parental consent have made it clear that the FTC routinely considers data security concerns and the possibility that a method may be

---

such as a password if they wish to change their choice later); *see also* 1.81.5 Cal. Civ. § 7025(7) (illustrative examples requiring a business to recognize prior consent choices when an individual changes devices or browsers). Any operator who insists on requiring a parent to grant consent separately on a new device should carefully consider whether this complies with G.B.L. § 1504 and does not impose an unfair burden on parents and covered minors.

circumvented, subject to fraud, or misused.[82] The proposed rule makes clear that the covered operator is best-placed to assess how users and third-parties interact with a method, and thus must reasonably consider the potential for circumvention, fraud, and misuse of the method it chooses to implement.

Allowing a covered operator who has already implemented a COPPA-compliant method for verifiable parental consent to rely on the same method with limited clarificatory requirements reduces the covered operator's burden of implementation and creates a streamlined and effective experience for its users. As described in Part III.B, the FTC has approved eight methods for verifiable parental consent as satisfying the requirements for COPPA and until now, these methods have set the standard for parental consent in the online environment. The methods have been widely adopted for online platforms directed to or having actual knowledge of users who are under the age of 13.

The OAG has carefully considered the use of verifiable parental consent methods approved by the FTC under the COPPA Rule for an online platform that is not governed by COPPA. Such methods have been reviewed and approved by the FTC at varying times over nearly three decades (starting with the first version of the COPPA Rule, issued in 1999), and reflect the different technologies available at the time. While a method may still be viable today, it is neither practical nor helpful in encouraging technological innovation to limit covered operators to only these methods. In addition, changing technology and user experiences may raise considerations about a given method that were not raised before the FTC at the time of approval.

Additionally, the FTC would not have considered any issues specific to minors aged 13 to 17, as this age group falls outside of the scope of COPPA. There are likely significant differences between the universe of minors under the age of 13 and the universe of minors aged 13 to 17. For example, minors aged 13 to 17 may be more likely to search for and be capable of carrying out ways to trick certain methods of verifiable parental consent, so the risk of circumvention and fraud may be higher than if the same method was used with minors under the age of 13.[83]

---

[82] *See, e.g.*, COPPA Rule, 90 Fed. Reg. at 16951-53 (discussing potential for types of fraud committed by child users using a verifiable parental consent method and misuse of data collected from the parent).

[83] For example, it may be more likely that a minor aged 13 to 17 is capable of setting up a VPN and separate email account to appear as if they are their own parent, compared to a minor under the age of 13. It is also possible using current technology to detect VPN use and to analyze data such as IP addresses and user activity to determine if two accounts likely belong to the same individual or are likely to belong to separate individuals. *See* Declaration of Tony Allen, *Free Speech Coalition, Inc. v. Paxton*, 1:23-cv-00917, W.D. Tex, Dkt. No. 27-4, par. 45 (Aug. 11, 2023); see *also* Determining IP Addresses That Are Associated With Physical Location With New Occupants And

Accordingly, OAG does not propose that methods approved by the FTC under the COPPA Rule be automatically deemed satisfactory under the proposed rule. However, OAG also stresses that none of these methods are explicitly prohibited by the proposed rule. If a covered operator wishes to implement such a method and determines that the method can be implemented in a way that addresses each requirement of section 700.2(e), the covered operator will have satisfied their compliance obligations under the proposed rule.[84]

iv. Annual review of parental consent methods

In section 700.2(e)(7), OAG proposes that a covered operator must review and update any verifiable parental consent method at least annually to ensure continued compliance with the proposed rule. Available technology may and does change rapidly, and such changes may affect whether a method can satisfy the rule's requirements over time. For example, available technology may make it much easier for a covered operator to detect whether a covered minor is using a different device to pretend to be their parent, or for an unrelated third-party to access information submitted by a parent as part of the verifiable parental consent method without authorization. A covered operator should make reasonable efforts to monitor such trends and to review and update the verifiable parental consent method it initially chooses to implement, just as the covered operator would for any other platform feature.

C. Section 700.3 Prohibition of nighttime notifications

1. Default and exceptions

In section 700.3(a), OAG proposes a default prohibition of nighttime notifications from covered operators to covered users. The section also proposes two exceptions to the prohibition, both of which are the obligation of the covered operator to effect: either the covered operator must establish the covered user's adult status through an age assurance

---

Providing Advertisements Tailored To New Movers To One Or More Of Those IP Addresses, U.S. Patent No. 10,333,810 B1 (issued June 25, 2019).

[84] For example, one COPPA-approved verifiable parental consent method is for the parent to present a form of government-issued identification, which is then checked against the parent using facial recognition and a human reviewer to confirm the parent is the same individual as in the identification. 16 C.F.R. § 312.5(b)(2)(vii). A covered operator seeking to use this method for minors aged 13 to 17 would need to consider, at minimum, section 700.2(e)(6)(vi) of the proposed rule, requiring the covered operator to provide an alternative method that does not require a government-issued form of identification. Another COPPA-approved method is sending the parent an email "coupled with additional steps to provide assurances that the person providing the consent is the parent." 16 C.F.R. § 312.5(b)(2)(viii). A covered operator seeking to use this method for minors aged 13 to 17 would also need to consider, at minimum, section 700.2(e)(6)(i) of the proposed rule, requiring the covered operator to determine the parent's age status pursuant to section 700.4 of the proposed rule. For example, the covered operator may consider including in the email to the parent instructions on how to access an appropriate age assurance mechanism.

method consistent with the requirements of section 700.4 or, if the covered user is determined to be a minor (through actual knowledge as defined in section 700.4(a)), the covered operator must obtain verifiable parental consent that complies with the obligations in section 700.3(e).

Proposed section 700.3(b) makes clear that covered operators are not required to offer a method of parental consent to covered minors. Under this proposed framework, should a covered operator elect not to make a method of parental consent available, section 700.3(a)(2) would not be available to that covered operator as an exception to the default prohibition of nighttime notification and the covered operator would not be able to provide a nighttime notification to any covered minor.

2. Exemption

Section 700.3(c) excludes "exempt online platforms," which under the proposed definition in section 700.1, means online platforms with fewer than 5 million monthly active users or fewer than 20,000 monthly active users who are covered minors, measured in accordance with that proposed definition. Covered operators whose total monthly active users do not reach these thresholds are not required to comply with the proposed rule until such time as the threshold is reached or exceeded, so long as the applicable platform is not affirmatively marketed or primarily directed to minors.

The basis for this proposed exemption, described in Part III.B, applies to nighttime notifications insofar as compliance with the requirement in section 700.3(a) would require adoption of age assurance methods as well.

3. Parental consent

Proposed section 700.3(e) implements G.B.L. §§ 1501(4) and 1502, requiring OAG to promulgate rules "identifying methods of obtaining verifiable parental consent" to provide nighttime notifications. The OAG has proposed an identical rule to that proposed for obtaining parental consent to provide an addictive feed. The statutory language of G.B.L. § 1502 that requires parental consent is virtually identical to that of G.B.L. § 1501(B), so there is no ground for imposing a different set of parental consent requirements. Moreover, providing a consistent standard for obtaining parental consent across both platform features (addictive feeds and nighttime notifications) will streamline implementation for covered operators and allow them to provide simple, straightforward requests to consent to covered minors and parents.

Nothing in the proposed rule prevents a covered operator from making available tools to allow a covered minor or a parent from further restricting when and how notifications may be sent, or from making independent decisions pursuant to its own platform policies to restrict

certain notifications.[85]

D. Section 700.4 Actual knowledge of minor age status and age assurance methods

1. Background

a. Historical use of age assurance methods

The use of age verification has a long history grounded in established legal and cultural norms. New York State law age-restricts a variety of goods and services including the purchase of tobacco products, alcohol, firearms, lottery tickets, and a tattoo or body piercing.[86] In addition, proof of age, typically via government-issued identification, is required for numerous activities such as renting a car or hotel room, participating in bike-sharing, opening a bank account, and signing up for a cellular phone number.[87] In light of these requirements, showing government-issued identification to prove age to access these products is both common and expected, particularly for individuals at or just over the legal age limit.

In contrast, social media websites and apps allowing access to minor users historically have required little or no information about user age, even when collecting other identifying information about the user.[88] Where platforms have requested such information to comply with federal regulations under COPPA or other legal requirements, the standard form of request has been asking the user to self-declare as a certain age (e.g., asking the user to check a box stating "I am 13 years of age or older" or to sign terms of service containing a representation that the

---

[85] G.B.L. § 1501(7) states that "[n]othing in this section shall be construed" as preventing the covered operator's restricting, based on its own independent decisions, access to or availability of media that the covered operator finds objectionable based on any grounds. Since G.B.L. § 1501(4), which directs OAG to promulgate rules regarding parental consent for providing nighttime notifications as well as an addictive feed, is in the same section, it follows that G.B.L. § 1501(7) also applies to nighttime notifications.

[86] N.Y. Pub. Health Law Art. 13-F, § 1399-cc (tobacco sales); N.Y. Alco. Bev. Cont. Law § 65 (alcohol sales); N.Y. Penal Law § 265 (firearm possession and sales); N.Y. Tax Law § 1610 (lottery ticket sales); N.Y. Pub. Health Law Art. 4-A (tattoos and body piercing).

[87] *See, e.g.,* Budget.com, "What Do You Need to Pick Up Your Rental Car?" https://www.budget.com/en/help/usa-faqs/required-credentials*; H*yatt.com, General FAQs, *https://www.hyatt.com/help/faqs/reservations;* Arya Sundaram, *Citi Bike will implement age verification, NYC officials and Lyft say*, Aug. 16, 2025, https://gothamist.com/news/citi-bike-will-implement-age-verification-nyc-officials-and-lyft-say; Chase, "Acceptable Forms of Identification," https://www.chase.com/content/dam/chase-ux/documents/personal/checking/acceptable-forms-of-identification.pdf ; AT&T, "Use a government-issued ID to set up an account," https://www.att.com/support/article/my-account/000107985/.

[88]Ariel Fox Johnson, *U.S. Age Assurance is Beginning to Come of Age: The Long Path Toward Protecting Children Online and Safeguarding Access to the Internet*, Common Sense Media, September 30, 2024, at 3-4.

user is over 13) with no validation of that information requested or furnished.[89] Outside of formal age assurance methods, however, social media platforms often have allowed users to record their birthday and other milestone events that in many cases provided ample evidence of their actual age.[90] Only in the last few years have a few platforms begun to use age assurance methods to restrict aspects of the online experience for minors.[91] These initiatives have not resulted in uniform age checks for existing users, however, as they have continued to rely in large part on users' self-declared ages, which are "woefully ineffective" at accurately identifying underage users.[92]

b. Development of the age assurance industry

The now-established and burgeoning age assurance industry has tracked the growing demand for age assurance methods online. While verifying age with government-issued identification is a well-established and legally accepted practice, early iterations of the internet thrived on relative anonymity and low "friction" for those users able to access the internet, allowing them to frequent numerous platforms with minimal constraints.[93] In the earliest days of the internet, given the relatively limited access and novelty, with costly devices and the need for expensive telephone lines, age assurance methods were not prioritized by online platforms.

As the internet has matured and become nearly ubiquitous in the last decade, the uses for tools to learn and verify the age of users have increased exponentially–to backstop e-commerce transactions, to better direct advertising dollars, and to ensure trust and safety on platforms, among others.[94] In addition, as described further below, an increasing number of laws have been enacted that require age assurance methods to combat harms to minors

---

[89] *See, e.g.*, Noah Apthorpe, et al., *Online Age Gating: An Interdisciplinary Evaluation*, at 26, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4937328.

[90] *See, e.g.*, Yasir K., LinkedIn Article, "Birthdays, Milestones, and Social Networking Platforms: Celebrating in the Digital Age"; May 26, 2024, https://www.linkedin.com/pulse/birthdays-milestones-social-networking-platforms-celebrating-khan-z6gqf.

[91] *See, e.g.,* Erica Finkle, "Bringing Age Verification to Facebook Dating," Dec. 5, 2022, https://about.fb.com/news/2022/12/facebook-dating-age-verification. Notably, effective age assurance is not performed on all Facebook Dating users, instead it is deployed only if the platform "detect[s] someone may be under the age of 18 and trying to use Facebook Dating." *Id.*

[92] Christine Marsden, *Age Verification Laws in the Era of Digital Privacy*, 10 Nat'l Sec. L.J. 210 (2023), at 227; *see also* Apthorpe, et al., n.89 *supra*, at 21 (referring to self-declaration as "security theater").

[93] Johnson, n.88 *supra*, at 6.

[94] Johnson, n.88 *supra*, at 7.

associated with the now nearly unlimited access to online platforms. This demand has, over time, given rise to a growing market for online age assurance methods.

c. Today's age assurance market

In response to the ANPRM, OAG received feedback on age assurance methods from a variety of stakeholders, including social media platforms, age assurance providers, trade associations, advocacy groups, and policy organizations. The OAG also has reviewed industry and academic research, laws and policies of governments outside the U.S., the results of third-party testing, certification standards, and economic analyses. Based upon this information, OAG can confirm that today, the age assurance market includes a robust variety of products that perform at a high accuracy rate, easily integrate with online platforms, handle large user volumes, and prioritize the preservation of user privacy and protection of user data. Age assurance products can be selected and customized to meet different business models, user populations, and compliance obligations. Age assurance providers are already servicing clients in the U.S. and globally, including many of the largest social media platforms, and are supported by a trade association, standards bodies, and providers of certification and testing.

OAG understands age assurance methods are not a one-size-fits-all solution and that the technology can and will continue to improve. Consideration of issues like data privacy, cost, and user burden must be essential to any technological evolution. These issues are well-known to the age assurance industry, which is actively engaged with governments, intergovernmental organizations, and other thought leaders worldwide to build and maintain solutions that balance the relevant public and private rights and interests.[95]

The proposed rule balances the interests of stakeholders to facilitate the adoption of effective age assurance methods while minimizing the associated risks and burdens. Current technology available in the age assurance industry offers options to covered operators for age assurance methods capable of meeting the proposed standards and OAG expects those options to expand as the technology advances to meet the growing demand for age assurance methods online.

2. Age assurance concepts

The following foundational concepts are important to understand how age assurance methods can be applied effectively. The most fundamental of these concepts is that age assurance methods do not require an individual to be identified—by name, birth date, or other demographics. While some age assurance methods use identification that includes some or all

[95] *See, e.g.,* Summit Communiqué Final, Global Age Assurance Standards Summit, May 22, 2025, https://accscheme.com/wp-content/uploads/Summit-Communique-Final-Document-May-2025.pdf.

of this information, it is by no means required by age assurance methods generally or to meet the standard in the proposed rule.

a. Age estimation and inference

Age verification via identification, both in-person and online, is a well-established method. It is generally considered to be the most accurate type of age assurance method at this time.[96] For many users, it is also considered burdensome, and for some it raises data privacy and security concerns.[97] Fortunately, new categories of effective online age assurance methods have emerged. Both age estimation and age inference lower user burden by determining a user's age using data more readily accessible than government-issued identification. Whereas historically, accessing an age-restricted good or service required traveling to the site where the good or service was offered and then physically furnishing identification for inspection upon demand, online users today who are asked to complete an age assurance method do not even need to cross the room to fetch identification.

Through age estimation, an online platform can analyze data from a user's physical features, through, for example, a "selfie" photo of the user's face, to determine whether the user meets the applicable age limit. This offers the advantage of requiring only information immediately accessible by users. Early trials of facial age estimation have shown it to be the overwhelming preference of users when presented as an option alongside age verification by identification.[98]

Age inference relies on documented data about the user that can be an analyzed to show the user is at or above a target age. This can be data already available to an online platform, such as the user's behavior on that platform, or data that can be accessed using basic information like a validated email address or cell phone number.[99] If the platform already has

---

[96] *See, e.g.*, Jim Siegl & Bailey Sanchez, *New FPF Infographic Analyzes Age Assurance Technology & Privacy Tradeoffs*, Future of Privacy Forum, June 26, 2023, https://fpf.org/blog/new-fpf-infographic-analyzes-age-assurance-technology-privacy-tradeoffs.

[97] *See, e.g., id*; Johnson, n.88 *supra*, at 10.

[98] *See, e.g.*, Rob Thubron, *Meta is bringing face-scanning age identification tech to Facebook Dating*, Techspot, Dec. 6, 2022, https://www.techspot.com/news/96869-meta-bringing-face-scanning-age-identification-tech-facebook.html (noting that Meta reported 81% of users asked to undergo age assurance chose facial age estimation over age verification using government-issued identification).

[99] Email or cell phone age inference is the comparison of a user's email address or cell phone against external data sources to find indicia of adulthood such as association with a utility bill or mortgage. *See* Verifymy White Paper, "Innovative age assurance: Email address as the new benchmark for frictionless age estimation," June 2024, at 18 ("Verifymy White Paper"), https://verifymy.io/wp-content/uploads/2024/11/Verifymy-White-Paper-

access to the necessary data and appropriate consents, the user may not even be aware that the platform has confirmed their age status.

b. Age assurance "waterfalls"

In addition to the proliferation of new age assurance methods, online platforms are able to combine those methods to, for example, further reduce user burden or take advantage of cost-effective methods that may not be successful in assuring the age or age status of all users. Platforms can develop an age assurance program that includes multiple methods and defaults users to the method requiring the least user burden or cost, only advancing users to higher-burden or higher cost methods if the lower-burden option is unsuccessful. This is commonly referred to as successive validation or an age assurance "waterfall."

As one example of a waterfall based on commercially available options today, a platform could adopt three different age assurance methods: age inference, facial age estimation, and age verification via identification. The platform could then sequence the age assurance process to start by routing users through an age inference method that requires the user to furnish no data at all, instead using only the platform's existing data. If 60% of users can demonstrate age status through this minimally burdensome method,[100] the experience for that 60% is optimized for both the users and the platform. If the remaining 40% of the platform's users are then prompted to complete facial age estimation and 35% complete it successfully,[101] only 5% of a platform's users will, as a last resort, be asked to undergo age verification via identification.

Waterfalls allow for the maximum number of users to successfully complete an age assurance method while undergoing the minimum burden necessary per user or incorporating platform priorities such as cost or leveraging information the platform already has. Additionally, some age assurance providers offer ready-made waterfalls, in which the provider routes the

---

Innovative-age-assurance-Email-address-as-the-new-benchmark-for-frictionless-age-estimation.pdf*;* Age Verification Providers Ass'n, "Demonstrating methods of age assurance," https://avpassociation.com/demonstrating-methods-of-age-assurance/.

[100] Data reported by age assurance provider Verifymy reflects that operators can confirm adult age status for 75-88% of adult users age 18-29 via the users' email address, with no further age assurance necessary. *See* Verifymy White Paper, n.99 *supra*, at 18. Based upon this estimate, an assumption of 60% age confirmation via age inference is likely conservative.

[101] According to facial age estimation provider Yoti, "99% of phone users submitting a face image are successfully age estimated." Yoti Facial Age Estimation White Paper, July 2025, at 14, https://www.yoti.com/wp-content/uploads/2025/09/Yoti-Age-Estimation-White-Paper-July-2025-PUBLIC-v1.pdf. Some adult users whose actual age is close to the target age may need to undergo additional age assurance if their adult age status cannot be confirmed by facial age estimation alone. S*ee id. at* 9.

user through age assurance methods from lowest to highest burden and in some instances charges no additional fees for subsequent methods.[102]

c. False positives and false negatives

No age assurance method in existence, including commonly accepted in-person methods, yields correct results 100% of the time. Understanding the accuracy of an age assurance method and comparing the accuracy of different age assurance methods and products are critical steps to ensuring covered operators build effective age assurance programs.

Testing of age estimation and inference methods typically measures three accuracy metrics:

- False positive rate: the number of users below the age limit who are falsely deemed to be at or above that limit and are incorrectly granted access to the restricted product or activity.
- False negative rate: the number of users at or above the age limit who are falsely deemed to be under the limit and thus are asked to undergo an additional age assurance method or are incorrectly denied access to the restricted product, potentially necessitating an appeal.
- Mean Average Error: the average distance between the user's age as calculated by the method and the user's actual age. This metric can help measure the improvement of a product over time.

Age assurance providers typically make this data available to platforms for evaluation and age assurance testing providers measure these metrics on an ongoing basis, as part of understanding a method's overall efficacy. A number of age assurance providers make their data available to the public.[103] For facial age estimation, these metrics also are measured by the National Institute for Standards and Technology ("NIST"), which currently publishes an ongoing

---

[102] *See, e.g.,* Verifymy, "Empowering users with optionality: The future of age verification and estimation," May 1, 2024, https://verifymy.io/blog/empowering-users-with-optionality-the-future-of-age-verification-and-estimation/; Incode, "Age Assurance Explained: Verification, Estimation, Segmentation, and Gating," July 8, 2025, https://incode.com/blog/age-assurance-explained-verification-estimation-segmentation-and-gating/. *See also* Bluecheck published rate sheet ("All data verifications," which include methods like cell phone-based age verification, "are only billed if the verification is successful"), updated May 22, 2024, https://docs.bluecheck.me/pricing.

[103] *See, e.g.*, Verifymy White Paper, n.99 *supra*; Yoti White Paper, n.101 *supra*.

study of facial age estimation methods, numbering 33 to date, with rolling admission for testing every three months.[104]

d. Data integrity and fraud prevention

While the furnishing of falsified data (e.g., a "fake ID") to support a customer's claim that they meet an established age limit is not a new concept, online age assurance methods must be built to address a host of unique challenges to protect the integrity of their results. For example, age estimation methods often include "liveness checks" to ensure that the images submitted are authentic and created by the same person whose age status is being sought. Where age checks require a user to submit email or cell phone data, that data is contemporaneously validated. And providers of online age assurance methods invest significant resources to stay ahead of the proliferation of AI-generated deepfakes, including by implementing technology that detects image manipulations and cybersecurity programs that protect against injection attacks.

e. Privacy protection and data deletion

Many online age assurance products have features and configurations that allow for data minimization and preservation of user privacy. They offer platforms the option of connecting via application programming interface and can determine and communicate a user's age status without sharing any other user data with the platform. Age assurance providers also can restrict the use of user data to the conduct of the age assurance method and once that age assurance method is complete, delete the data without storing it.[105]

Zero-knowledge proof age assurance solutions, also called "double-blind" age verification (*see* definition of "zero-knowledge proof age assurance," Part III.A) represent another option for an age assurance method that protects user privacy. While this method is not widely used today as an age assurance method, it is gaining traction as a maximally privacy-preserving method for users and has been a focus of efforts by both governments and the private sector to prioritize user privacy.[106]

---

[104] Kayee Hanaoka, et al., NIST Interagency Report: Face Analysis Technology Evaluation: Age Estimation and Verification, 12th Update (8-28-2025), https://doi.org/10.6028/NIST.IR.8525.

[105] *See, e.g.*, Yoti White Paper, n.101 *supra*, at 2 ("The images are not stored, shared, re-used or sold on. Images are immediately and permanently deleted according to GDPR best practice, and we do not use them for our own learning or training purposes").

[106] For example, the recent prototype released by the European Commission for age verification includes zero knowledge proofs. *See* European Age Verification Solution, Operational, Security, Product, and Architecture

f. Certification and testing

Certification and testing of age assurance methods play an important role in setting uniform standards in the industry and measuring individual providers and methods against those standards. Currently, two internationally recognized standards exist to test and certify age assurance methods: IEEE 2089.1 and ISO 27566. Both standards provide a framework for evaluating age assurance methods that include method accuracy, privacy and data minimization, and data security. Both also allow for customization based on method type and applicable legal requirements.

Nationally and internationally recognized standards can be used by private testing companies to test age assurance methods and certify compliance with the standards along with applicable laws and regulations. Testing is critical to evaluating age assurance methods against the uniform standards established by the standards bodies and the applicable legal requirements, particularly in light of legal mandates for live user data minimization and deletion. In particular, testing companies are able to apply test data sets, compiled in accordance with specifications from applicable law, to validate the accuracy of age assurance methods–including false positive, false negative, and mean average error rates. Testing also typically includes validation of data privacy and security practices.

g. Recent developments in online age assurance methods

i. Recent non-US laws, requirements and guidelines

In recent years, a number of countries have passed laws requiring platforms to implement age assurance methods or have issued age assurance-related guidance. These developments have strengthened the market for age assurance methods and hastened the establishment of uniform standards and transparent data regarding method effectiveness.

In the United Kingdom, effective as of July 25, 2025, the Online Safety Act requires platforms featuring pornography or other harmful or high-risk activities for minors to implement

---

Specifications, Annex B: Zero Knowledge Proofs for the Age Verification Solution, https://ageverification.dev/Technical%20Specification/annexes/annex-B/annex-B-zkp.

Google also recently announced the release of an open source zero knowledge proof age assurance model in connection with its digital wallet. *See* Alan Stapelberg, "Opening up 'Zero Knowledge Proof' technology to promote privacy in age assurance," July 3, 2025, https://blog.google/technology/safety-security/opening-up-zero-knowledge-proof-technology-to-promote-privacy-in-age-assurance/.

"highly effective" age assurance methods and to prevent minors from accessing the platform.[107] The UK Office of Communications ("Ofcom") has confirmed that highly effective age assurance methods include "photo ID matching, facial age estimation, mobile network operator age checks, credit card checks, digital identity services and email-based age estimation."[108]

In Australia, the Online Safety Amendment (Social Media Minimum Age) Act 2024 requires that, by December 2025, social media platforms take reasonable steps to block access for all minors under the age of 16.[109]As part of the development of regulations to implement this mandate, the Australian government commissioned a global age assurance trial, in which age assurance methods from 48 separate providers were tested and evaluated. The preliminary findings from this trial were released on June 20, 2025, including the overall conclusion that "age assurance can be done in Australia privately, robustly and effectively."[110] The final results, which were released on September 1, 2025, reflect the most comprehensive evaluation of online age assurance methods in history.[111]

As of April 11, 2025, in France all platforms offering pornography must offer a double-blind method of age verification to protect user privacy while ensuring minors do not have access to the site.[112] This updates the requirement, originally issued by the French government

---

[107] Department for Science, Innovation and Technology, Online Safety Act 2023, July 24, 2025, https://www.gov.uk/government/collections/online-safety-act.

[108] Ofcom, "Age Checks to Protect Children Online," Jan. 16, 2025, https://www.ofcom.org.uk/online-safety/protecting-children/age-checks-to-protect-children-online. While some additional methods cited by Ofcom would not currently be highly effective in the United States, such as an age assurance check based on open banking, many cited methods are equally or similarly effective in the United Kingdom and the United States.

[109] Samba Khan, "Australia: Social Media Banned for Children Under 16," Law Library of Congress, December 9, 2024, https://www.loc.gov/item/global-legal-monitor/2024-12-08/australia-social-media-banned-for-children-under-16.

[110] Tony Allen, Age Assurance Technology Trial Preliminary Findings Event, June 20, 2025, https://ageassurance.com.au/wp-content/uploads/2025/06/AATT-Preliminary-Findings-Event-20-June-2025.pdf.

[111] Age Check Certification Scheme, *Age Assurance Technology Trial Final Report*, Sept. 1, 2025, https://www.infrastructure.gov.au/department/media/publications/age-assurance-technology-trial-final-report.

[112] Arcom, Oct. 2024, "Reference setting out the minimum technical requirements applicable to age verification systems implemented for access to certain online public communication services and video-sharing platforms that make pornographic content available to the public" (translated); https://www.arcom.fr/sites/default/files/2024-10/Arcom-Referentiel-technique-sur-la-verification-de-age-pour-la-protection-des-mineurs-contre-la-pornographie-en-ligne.pdf.

in 2020, requiring adoption of age assurance methods beyond self-declaration by pornography platforms.

As part of the European Union Digital Services Act, which includes age assurance methods to protect children online, on July 13, 2025, the European Commission released a blueprint for an age verification solution.[113] This prototype, which is being released on an open-source basis, is intended as a stopgap solution pending the rollout of European Digital Identity Wallets in 2026.[114]

ii. Adoption of Age Assurance Methods by Social Media Platforms

In the last six months, alongside new laws mandating age assurance methods and an increase in public dialogue around online harms to children, social media platforms have been implementing various new forms of age assurance methods. Recent examples include:

- X has announced the use of email age inference and age inference using social connections as an age assurance method in the United Kingdom, for users who attempt to view pornography;[115]
- Discord is trialing facial age estimation in the United Kingdom and Australia;[116]
- Bluesky is using facial age estimation, ID verification, and payment card verification to age-gate mature content and direct messaging in the United Kingdom;[117]

---

[113] European Commission, "The EU Approach to Age Verification," https://digital-strategy.ec.europa.eu/en/policies/eu-age-verification.

[114] European Commission, "Commission makes available an age verification blueprint," July 14, 2025, https://digital-strategy.ec.europa.eu/en/news/commission-makes-available-age-verification-blueprint.

[115] Mark Sellman, *X to block children from watching porn by checking email address*, The Times, July 24, 2025, https://www.thetimes.com/article/3f988f21-1202-4799-8668-84fdc495eead.

[116] Imran Rahman-Jones & Chris Vallance, *Discord's face scanning age checks 'start of a bigger shift,'* BBC, April 17, 2025, https://www.bbc.com/news/articles/cjr75wypg0vo.

[117] Emma Roth, *Bluesky is rolling out age verification in the UK*, The Verge, July 10, 2025, https://www.theverge.com/news/704468/bluesky-age-verification-uk-online-safety-act.

- Instagram has implemented facial age estimation and ID verification in connection with the rollout of teen accounts[118] and is developing AI-based age inference technology to identify teen users that are mis-classified as adults;[119]
- Roblox has announced the rollout of age assurance via facial age estimation or ID verification for users who wish to use text or chat tools;[120]
- Google offers ID and credit card age verification in the United States and additionally offers email age inference in the UK;[121] it also announced in July that it would begin deploying AI to perform age inference on U.S. users of Google products, including YouTube, and would prompt users flagged as potential minors to perform facial age estimation or ID verification.[122]

The incorporation of age assurance methods into the infrastructure of social media platforms is a positive development that demonstrates the technical and financial feasibility of age assurance methods for these platforms. Unfortunately, voluntary adoption of age assurance methods has not achieved the level of protection of minors required by the Act. The aforementioned steps are being applied by a limited number of platforms and in many cases, only in select countries in response to the implementation of legal requirements. Other platforms are only triggering age assurance methods in limited circumstances, such as when the platform is alerted by another user that a minor may be misclassified as an adult. Not only is this approach to age assurance not comprehensive enough in scope, but also, once minors are identified, the measures implemented by some platforms to curb harm to those minors (where

[118] Instagram help page, "Confirming your age on Instagram," https://help.instagram.com/966909308115586/?helpref=related_articles.

[119] Barbara Ortutay, *Instagram tries using AI to determine if teens are pretending to be adults*, Associated Press, April 21, 2025, https://apnews.com/article/instagram-teens-parents-age-verification-meta-94f1f9915ae083453d23bf9ec57e7c7b.

[120] Robert Booth, *Roblox to extend age checks in attempt to curb adults talking with children*, The Guardian, Sept. 3, 2025, https://www.theguardian.com/games/2025/sep/03/roblox-age-checks-adults-children-safety.

[121] Google Account Help, "Access age-restricted content & features," https://support.google.com/accounts/answer/10071085.

[122] Jennifer Elias, *Google to test using AI to determine users' ages*, CNBC, Feb. 12, 2025, https://www.cnbc.com/2025/02/12/google-to-test-using-ai-to-determine-users-ages.html.

implemented at all) have, thus far, demonstrated limited efficacy.[123] And no platform has publicly announced a voluntary plan to eliminate its addictive feeds for minor users.

3. OAG framework for implementation of age assurance methods

The Legislature made clear that to provide an addictive feed, addictive online platforms must take affirmative action—they must use commercially reasonable and technically feasible methods to determine that a covered user is not a covered minor. G.B.L. § 1501(2) authorizes OAG to promulgate regulations identifying such methods and any exceptions thereto based on factors listed in G.B.L. § 1502(2)(b). Those factors are the size, financial resources, and technical capabilities of the addictive online platform, the costs and effectiveness of available age determination techniques for users of the addictive online platform, the audience of the addictive online platform, prevalent practices of the industry of the covered operator, and the impact of the age determination techniques on the covered users' safety, utility, and experience. Having considered the factors, OAG proposes section 700.4, which outlines the elements of age assurance methods and related requirements proposed by OAG. An explanation of the proposed requirements follows.

a. Actual knowledge of minor age status

The OAG recognizes that many covered operators already have reliable information about their existing minor users' age or age status or may come into such information through reliable channels other than age assurance methods. Under some circumstances, this information may qualify as actual knowledge of minor status and render age assurance methods unnecessary for the corresponding users. As the intent of the Act is to protect minors—including those minors that lie about their age to online platforms when given the opportunity — meeting G.B.L. § 1502(2)(b)'s requirement of determining that a covered user is not a covered minor requires diligence and a level of confidence about a user's adult status on the part of the covered operator.

If a covered user self-declares as a minor, either in response to a request by the covered operator or in any other form that allows the covered operator to reasonably associate the declaration with the covered user, that self-declaration constitutes actual knowledge of minor age status by the covered operator under proposed section 700.4(a)(1). Self-declaration as an adult, given its well-documented susceptibility to falsification, is not an acceptable age assurance method under the proposed rule.[124] But under proposed section 700.4(a)(1), covered

---

[123] Geoffrey A. Fowler, *Gen Z users and a dad tested Instagram Teen Accounts. Their feeds were shocking.,* The Washington Post, May 18, 2025, https://www.washingtonpost.com/technology/2025/05/18/instagram-teen-accounts-test/.

[124] *See, e.g.*, Johnson, n.88 *supra,* at 9*;* Apthorpe, *et al.*, n.89 *supra,* at 21; Marsden, n.92 *supra*, at 227.

users who self-declare as minors do not need to undergo the burden of additional age assurance methods. Allowing self-declaration as a minor upholds the statute's legislative purpose of protecting minors and additionally reduces user burden and operator cost. Notably, nothing in this section prevents a covered operator from requesting that a self-declared minor undergo age assurance methods for reasons unrelated to compliance with the proposed rule, including to enforce the covered operator's trust and safety policies or to comply with other legal or regulatory obligations.

The OAG also is aware that some covered operators collect data on covered users for the platforms' commercial benefit. For example, the platform may use data sufficient to conclude a covered user's age or age status to sell targeted advertisements directed to that covered user. In the event this data is maintained by the covered operator for marketing, content selection, or other commercial purposes and would be sufficient to conclude the covered user's minor status if applied to an age assurance method offered by the covered operator, the covered operator has actual knowledge of the covered user's minor status under proposed section 700.4(a)(3). This provision ensures covered operators cannot commercialize information about the user's minor age status while claiming ignorance of that age status for purposes of compliance with the proposed rules. At the same time, merely possessing data about a user without the ability to discern the user's age status from that data does not implicate this requirement.

Finally, the covered operator may receive other, reliable evidence of a covered user's minor age status. Examples may include a credible report from another user or the family member of a covered user. Where the covered operator is able to make a good faith determination that this information indicates minor age status, the covered operator has actual knowledge of that status.

b. Categories of acceptable age assurance methods

Consistent with the statutory mandate that OAG identify "commercially reasonable and technically feasible methods for a covered operator to determine if a covered user is a covered minor,"[125] OAG reviewed comments in response to the ANPRM and consulted data and stakeholders regarding age assurance methods, including how they operate, commercial applications, how third-party age assurance methods integrate into other platforms, and the effectiveness of different methods at determining minor age status. The OAG also solicited and received stakeholder feedback regarding the optimal framework for implementation by platforms with addictive feeds.

Considering all available information and data, OAG has concluded that three categories of age assurance methods can effectively determine a covered user's age status consistent with

[125] G.B.L. § 1501.2(a).

the applicable accuracy minimums if certified in accordance with the requirements in section 700.5. Those three categories are age verification, age estimation, and age inference. Each of these categories includes multiple age assurance methods that are commercially available today as well as methods still in development that may provide effective and privacy-preserving age assurance in the future.

The OAG considered whether to propose regulations that endorse or otherwise specify a list of compliant age assurance methods or providers. The OAG preliminarily concludes that general categories of age assurance methods create a preferable construct for covered operators and users, for several reasons. First, there is no one age assurance method that fits all applications. The proposed rule allows covered operators the flexibility to create a framework that best integrates age assurance methods with its existing user experience and meets the needs of its user population. In addition, the efficacy of a method is heavily dependent upon how it is operationalized by the covered operator. It is also the case that age assurance methods are consistently improving and new methods are becoming available in response to increasing demand. The OAG wishes to facilitate a robust market for age assurance methods rather than place limitations on acceptable methods.

While the three allowable age assurance method categories include virtually every commercially available age assurance method, a few methods historically used by platforms are excluded from these categories. Among these unallowed methods are self-declaration as an adult by the covered user and written confirmation of adult status, referred to as "vouching," by a third-party without documentary or other supporting evidence. These methods do not constitute age assurance methods as defined by the proposed rule and generally lack reliability.[126]

c. Age assurance accuracy requirements

The OAG proposes maximum allowable false positive rates (i.e., the rate of minors falsely determined to be adults) for age assurance methods and minimum detection rates for method circumvention, to identify age assurance methods that are effective in determining a covered user is not a covered minor. Setting false positive rates gives covered operators flexibility while ensuring that age assurance programs are serve the Act's goal of protecting minors. This flexibility also allows operators to optimize user experience while taking into account the availability of age assurance methods and products and their current accuracy rates. The proposed maximum false positive rates plus method circumvention detection rates are identified in the proposed rule as the "accuracy minimum" and the "total accuracy minimum."

[126] Johnson, n.88 *supra,* at 9*;* Apthorpe, *et al.*, n.89 *supra,* at 21; Marsden, n.92 *supra*, at 227.

These minimums create a uniform standard for covered operators to use to evaluate and adopt age assurance methods.

d. Accuracy minimums by age group

Both the accuracy minimum and total accuracy minimum contain maximum false positive rates broken down by age category, with requirements divided into ages 0-7 (.1%), 8-13 (1%), 14-15 (2%), 16 (8%), and 17 (15%). The OAG proposes these age categories based on its review of accuracy data across a variety of age assurance methods, in addition to general information on age assurance method function and accuracy.[127] For many age assurance methods, accuracy increases in relation to the size of the age difference between the user and the target age. In other words, a single age assurance product might almost always identify a 13-year-old as a minor but is likely to be less consistently correct for 17-year-olds, some of whom may be just a few weeks or months from reaching adult status.[128]

The OAG considered proposing a single false positive threshold for all minors but proposes difference thresholds by age category because OAG believes the latter would avoid certain undesirable outcomes. For example, if the maximum false positive rate allowed in the proposed rule were too low, e.g., 1% for all minors regardless of age, a substantial number of age assurance methods would not currently be able to reach the accuracy minimum for the users closest to 18. Operators would not be able to take advantage of the methods that are otherwise highly effective at separating the vast majority of minors from adults. This outcome is inconsistent with the OAG's policy objectives of encouraging a robust age assurance market and choice for covered operators and users.

Conversely, a higher proposed false positive rate, e.g., 15% for all minors regardless of age, would enable more age assurance methods to meet the threshold but also would allow

---

[127] The OAG consulted sources including the *Ofcom Guidance on highly effective age assurance and other Part 5 duties*, January 16, 2025, https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/guidance-on-highly-effective-age-assurance-and-other-part-5-duties.pdf; NIST face analysis technology evaluation, n.104 *supra*; the Verifymy and Yoti White Papers, n.99 & n.101, *supra*; the Age Check Certification Scheme Global Age Assurance Standards Summit, *see* n.95, *supra*; and the materials produced by the Age Check Certification Scheme in the conduct of the Australia Age Assurance Technology Trial, *see* n.111 *supra*. The OAG also considered all comments submitted in response to the ANPRM.

[128] Siegl & Sanchez n.96 *supra*; *see also* Future of Privacy Forum, *Unpacking Age Assurance: Technologies and Tradeoffs*, Infographic, https://fpf.org/wp-content/uploads/2023/06/FPF_Age-Assurance_final_6.23.pdf. Notably, this paradigm is also true for in-person age assurance methods: an individual whose actual age is close to the target age and who may appear to be at or above the target age is less likely to be asked to provide identification in order to access an age-gated product or service.

more underage users to be falsely treated as adults than is necessary given the effectiveness of the technology in identifying the youngest users as minors. These users arguably need the most protection and can be robustly protected—as reflected in the proposed rule—with current technology.

Breaking the accuracy minimum down by age category thus reaches the best overall outcome by requiring near-perfect results for the youngest users and tailoring the minimums to allow still-high but lower accuracy rates for users who are closer to adult status.

e. Accuracy minimum and total accuracy minimum

The OAG proposes both an accuracy minimum and a total accuracy minimum as thresholds for age assurance methods to balance the goals of accuracy, method availability, and optimal user experience. The two proposed standards interact as follows: every age assurance method offered by a covered operator must meet the accuracy minimum. This requirement ensures that covered operators are relying on methods that are only rarely mis-identifying minors as adults. The formula for calculating the accuracy minimum includes correct and incorrect results but excludes inconclusive age assurance outcomes, *i.e.*, when the method cannot determine an individual's age or age status. The practical effect of this exclusion is that covered operators may choose age assurance methods that offer benefits such as very low user friction and have low false positive rates but are not able to make a determination for some users, even perhaps a large percentage. One such example is email age inference, which is a low-friction method that can generate low false positive rates, but which can reach an inconclusive result for a non-trivial percentage of users, depending upon the user population.[129]

The total accuracy minimum is the same as the accuracy minimum in all respects except that inconclusive age assurance outcomes are included in the calculation of the total accuracy minimum along with incorrect results. While all age assurance methods offered must meet the accuracy minimum, only one method offered by a covered operator must meet the total accuracy minimum. That one method is sometimes referred to as the "method of last resort" by age assurance providers. Requiring one method that meets the accuracy minimum inclusive of inconclusive age assurance outcomes maximizes the likelihood that the standard for the accuracy minimum can be met for all users as a whole.

---

[129] Email age inference generates inconclusive results when an email address cannot be confirmed as associated with data indicating adulthood. While this lack of association may indicate that the user is not an adult, it also may be due to an email address being relatively new or not the primary address for the user, or the user having a smaller digital footprint. *See* Verifymy White Paper, n.99 *supra*, at 17. The inability to definitively state that a user is not an adult may not allow an age assurance method to meet the total accuracy minimum; however, it still may be a highly effective method for identifying adult users with minimal friction.

By defining and proposing operators' age assurance methods be subject to an accuracy minimum for all methods and a total accuracy minimum for at least one method, the proposed rule requires high accuracy standards that can apply to all users while increasing the number and combination of age assurance methods that covered operators can access to achieve a compliant, cost-effective, individualized, and burden-minimizing age assurance program.

f. Prevention of method circumvention

Prevention of method circumvention is critically important to accomplishing the primary objective of protecting minor users. Particularly given the proliferation of AI-generated false information and the speed at which strategies can be shared by users online, covered operators and their agents must remain constantly vigilant to stay one step ahead of efforts to undermine the integrity of age assurance methods. To ensure these efforts remain robust at all times, OAG proposes to include in the definition of "accuracy minimum" and "total accuracy minimum" a requirement that the age assurance method detect 98% of all attempts at method circumvention. This proposed requirement will limit the age assurance methods offered by a covered operator to those that consistently and effectively detect attempts to submit false information or otherwise undermine age assurance.

In addition to the 98% detection requirement, which would be confirmed via annual testing and certification, OAG also proposes a requirement at section 700.4(d)(3) that covered operators monitor changes in aggregate age assurance outcomes (via the data related to those outcomes, collected in accordance with section 700.7) and act on reports, both directed to the operator and shared publicly, that indicate new or previously undetected forms of method circumvention on the operator's platform. If the data or reports validate the use of a new or previously undetected method by a material number of users, the covered operator must take steps to correct any associated false positive determinations and also must take steps to effectively detect such forms of method circumvention going forward. This obligation is intended to prevent the rapid proliferation of new forms of method circumvention via information shared by users online, which has the potential to quickly reduce a covered operator's detection rate well below 98%.

Covered operators or agents that detect method circumvention by a covered user may offer the covered user the opportunity to present accurate data. The covered operator should only offer a very limited number of attempts to correct an original submission of false data, however. In the absence of a prompt, good-faith effort by a user to correct falsified data, the covered operator should assume that the user is a covered minor.

g. Covered operator flexibility

Within the proposed accuracy thresholds, a covered operator can construct an age assurance program that best meets its business objectives and the needs and preferences of its

users. Some covered operators may choose to offer only the minimum number of age assurance methods to meet the obligations in the proposed rule. Other covered operators might choose to maximize the choice of age assurance methods offered to users. Still others might construct an age assurance waterfall in which multiple age assurance methods are offered but the sequence of methods presented to covered users is pre-selected to minimize user friction.

For some covered operators that already have substantial user data, applying this data to an age assurance method that meets the proposed standard (with the user's valid consent) might be a logical first step to minimize any burden associated with age assurance methods for existing users. Other platforms might need or prefer to route all current and future users through a uniform age assurance flow. Under the proposed rule, any number of age assurance programs, offering age assurance methods alone or in combination, are possible so long as the covered operator meets the requirements of proposed section 700.4.

h. Default adult age status

Consistent with the proposed accuracy minimum and total accuracy minimum requirements, a covered operator's age assurance program generally should yield a determination of adult or minor age status for a substantial majority of covered users. In the event a user undergoes an age assurance method and the result is inconclusive, the covered operator should prompt the user to proceed to an alternative method.

If the covered user completes all age assurance methods offered by the covered operator, including at least one method that meets the total accuracy minimum, and the result of each method is inconclusive, then pursuant to proposed section 700.4(b)(1)(ii), the covered operator may presume the covered user has adult age status so long as the covered operator otherwise has no actual knowledge of minor age status for the covered user. This presumption may persist until such time as the covered operator receives information that conveys actual knowledge of minor age status pursuant to proposed section 700.4(a).

i. Requirements for age verification via identification

Under G.B.L. § 1501(2)(c), the rules implementing the age assurance method requirement in the Act must ensure covered operators provide "at least one method that either does not rely solely on governed issues identification or that allows a covered user to maintain anonymity as to the covered operator." Presenting government-issued identification can present unique concerns regarding equity as among users, some of whom may not have government-issued identification, and user data privacy, as reflected in stakeholder feedback in response to the ANPRM as well as related academic research and industry publications.[130] Proposed

[130] *See, e.g.*, Siegl & Sanchez, n.96 *supra*; Johnson, n.88 *supra*, at 9.

sections 700.4(c)(1), 700.4(c)(2), 700.4(c)(3) implement the Legislature's mandate in G.B.L. § 1501(2)(c). First, section 700.4(c)(1) makes clear that covered operators using government-issued identification for an age assurance method must accept government-issued identification from all U.S. and non-U.S. jurisdictions. This ensures maximum access for users who can demonstrate adult age status and is already part of the age verification services many age assurance providers provide because their services are increasingly used around the world.

Second, per proposed section 700.4(c)(2), a covered user that declines to provide government-issued identification upon request must be allowed to proceed to the appeals process outlined in proposed section 700.6. This allows covered users with privacy concerns related to sharing their identification an alternative method of demonstrating their adult age status but also ensures that covered operators remain obligated to obtain reliable evidence that conveys actual knowledge that the user is not a covered minor prior to classifying the user as an adult. Pursuant to section 700.6(a)(1), the appeals process must allow for the submission of at least one type of documentation other than government-issued identification.

Third, under proposed section 700.4(c)(3) covered operators either must offer at least one age assurance method other than age verification from a government-issued identification or must offer a zero-knowledge proof age assurance method, which will protect the privacy interests of the covered user. Consistent with G.B.L. § 1501(2)(c), OAG proposes to define and expressly allow zero-knowledge proof age assurance. If implemented and used properly, it is a privacy-maximizing solution utilizing the high accuracy of identification-based age verification.

j. Investigations and changes in status

Under proposed section 700.4(d)(2), if a covered operator receives a report or information indicating that a covered user classified as an adult has minor age status, the covered operator has an obligation to conduct an investigation sufficient to determine whether the new information constitutes reliable evidence of minor status that conveys actual knowledge pursuant to section 700.4(a)(4). Recognizing the obligation under G.B.L. § 1501(2)(b) that, even with the implementation of effective age assurance methods, not every covered user will be correctly classified in the first instance, OAG proposes requiring investigation of information subsequently presented to or discovered by a covered operator regarding a covered user's age status. This requirement makes clear that while the covered operator is entitled to rely upon the results of an age assurance method that meets the requirements of section 700.5, the covered operator also has an ongoing obligation investigate information in its possession that may be sufficient to constitute actual knowledge of minor age status. This includes information used by the covered operator for commercial purposes, pursuant to proposed section 700.4(a)(3), subsequent to a covered user's adult age status determination.

Under proposed section 700.4(d)(1), should the covered operator obtain actual knowledge of a covered user's minor age status after initially classifying the covered user as an

adult, the covered operator must re-classify the user as a covered minor within 10 business days. This requirement allows the covered operator a reasonable time period to change its classification but also ensures that an erroneous determination of adult status is corrected in a timely fashion to limit harm to the minor on a go-forward basis.

The OAG also proposes section 700.4(d)(4) under which covered operators must offer covered users classified as minors a method to change that self-declaration when they reach adult status. Eventually, covered minors will be entitled to be classified as adults and proposed 700.4(d)(4) requires the operator to have a process by which covered minors can change their status. Because self-declaration as an adult is not sufficient to convey actual knowledge of adult age status, covered users who change their age status must then undergo an age assurance method before the covered operator can treat them as covered adults.

k. User notice and design features

The proposed rule includes two provisions designed to improve transparency regarding age assurance methods for covered users and reduce the potential for user confusion or misdirection. First, proposed section 700.4(e) requires covered operators to provide covered users with an explanation of the age assurance method(s) offered, including, with respect to any request for user data, "the purpose of the data request, how the data will be used, and when and how the data will be deleted." The user notice requirement is intended to increase covered users' awareness of how age assurance methods work and why the requested data is necessary to effect it. The notice also is intended to explain the covered operator's obligations regarding handling of user data to proactively address user concerns about data privacy and security.

Second, section 700.4(f) prohibits covered operators from introducing any design feature "that discourages covered users from participating in or successfully completing an age assurance method or facilitates the falsification of data or method circumvention by covered users." This requirement recognizes the responsibility of the covered operator to integrate age assurance methods into its user interface and is intended to prevent any intentional or unintentional design decisions by the covered operator that frustrate the user's ability to successfully complete the age assurance process. Additionally, any attempt by a covered operator to intentionally allow or encourage a covered user to engage in method circumvention, for example by submitting falsified data, would violate this section. For example, a user interface allowing users numerous attempts to undergo an age assurance method while disregarding evidence of data falsification may allow users to engage in method circumvention, and as such is prohibited.

l. Periodic evaluation and future improvements

While the proposed rule offers covered operators the ability to customize an age assurance program provided the methods meet the accuracy minimums, OAG also recognizes

that choices made by the covered operators in designing an age assurance program will directly impact the overall effectiveness of the age assurance methods and level of burden to covered users. This includes the adoption of age assurance methods with high false negative rates (i.e., adults wrongly identified as minors) which, while not prohibited or limited by the proposed rule, can create unnecessary burden for adult users. The requirement proposed in section 700.4(g) makes clear that covered operators should consider the impact of chosen age assurance methods on both accuracy and user burden, and that this obligation is an ongoing part of the maintenance of an age assurance program.

The OAG also is aware that age assurance methods are consistently improving and increased adoption of these methods around the world is likely to further catalyze improvement and innovation in the industry. Technology to detect method circumvention also is constantly evolving and improving. As a result, the false positive rates and method circumvention detection rate cited in the accuracy minimum and total accuracy minimum, which today reflect highly effective age assurance methods, may one day represent a lower benchmark than the industry standard. The OAG will continue to monitor progress in the age assurance industry and may amend the proposed rule via future rulemaking to conform the accuracy minimums to improved performance across age assurance methods. But under the proposed rule, covered operators also should remain apprised of the evolving performance of age assurance methods, including new and innovative methods, and should update their age assurance program to adopt methods that lower both false positive and false negative rates and improve method detection rates consistent with the Act's mandate to account for user safety, utility, and experience.

4. Commercial reasonability and technical feasibility

In accordance with its statutory mandate to promulgate regulations "identifying commercially reasonable and technically feasible methods" for age assurance,[131] in creating the proposed age assurance framework in section 700.4, OAG closely considered the commercial reasonability and technical feasibility of each requirement. As described below, based on today's age assurance market, the adoption of an age assurance method or methods sufficient to meet the accuracy minimums is both commercially reasonable and technically feasible for platforms with addictive feeds unless they meet the definition of an exempt addictive online platform.

a. Commercial reasonability

As detailed in the economic analysis in Part IV, the cost of implementing and maintaining age assurance methods in compliance with the proposed rule is commercially reasonable for

[131] G.B.L. § 1501.2(a).

covered operators. While covered operators have the option of developing in-house age assurance technology and some providers may already be doing so, today's age assurance industry includes numerous third-party providers capable of complying with the requirements of the proposed rule, that covered operators can engage to perform age assurance methods on their behalf.

Third-party age assurance methods are technically sophisticated, with many involving machine learning, and can perform at a large scale. The age assurance industry offers choice to covered operators and the number of market players and scalability of the technology fosters price competition that keeps service fees stable and relatively low, particularly for operators able to offer high user volumes (the economic analysis estimates an average of $0.15-$0.30 per user for age checks before volume discounts). The OAG's preliminary analysis based on conservative assumptions, estimates the all-in cost of implementing and maintaining age assurance methods amounts to be less than two percent of even a smaller covered operator's operational costs and the impact for larger platforms is exponentially smaller.

Additionally, the relative ease with which many age assurance methods can be completed, with limited or in some cases no burden on the covered user, means the impact on user engagement will not be material. Moreover, competitors will be similarly impacted. And while the expected changes in the online behavior of covered minors resulting from the discontinuation of addictive feeds will impact the extent of covered operators' monetization of minor users' engagement, the scale of that impact based on minor users in the State of New York is quite small, particularly compared to the substantial volumes of advertising revenue reported by large social media platforms. In sum, based on the information available to OAG, there is no reason to conclude the cost or commercial impact of implementing age assurance methods will make the adoption commercially unreasonable for covered operators (with exception of exempt addictive online platforms, as discussed below).

b. Technical feasibility

Implementing age assurance methods in today's market also is technically feasible; this is well-demonstrated by the increasing adoption of age assurance methods by large companies like Meta and Google (as described above). Age assurance methods are no less technically feasible for smaller covered operators. Most age assurance providers offer integration via application programming interface or software development kit and integration does not require specialized resources.[132] Additionally, many age assurance providers transmit age

[132] Age Check Certification Scheme, *Age Assurance Technology Trial Practice Statements - Age Verification, A-5.1.2,* May 21, 2025, https://ageassurance.com.au/wp-content/uploads/2025/06/Practice-Statements-for-Age-Verification.pdf; *see also* United Kingdom Department for Science, Innovation & Technology, Online Safety Act:

assurance results without sharing any underlying user data, eliminating the need for the data to be maintained or protected by the covered operator. Under the proposed rule, covered operators also can customize their user interface to incorporate age assurance methods in the manner best suited to their existing user experience.

Additional technical requirements are minimal; primarily, the covered operator must use available data and take reasonable steps to determine whether a user is a covered user and to detect user efforts to conceal or misrepresent the user's location, as described in Part III.B. With the limited exceptions noted below, these tasks are well within the technical capabilities of covered operators.

E. Section 700.5 Certification of age assurance methods

1. Annual certification

Certification plays a key role in establishing and enforcing standards for the critical aspects of age assurance methods including accuracy, data privacy, and data security. Proposed section 700.5(a) requires covered operators to obtain annual certification for each age assurance method it offers. The OAG considered different certification frequencies, including for age assurance methods with a consistent history of past certifications. Ultimately OAG concluded that an annual cadence balances the relative burden of undergoing testing and certification with maintaining the integrity of the age assurance process in light of the frequency with which age assurance methods are being updated, and in particular, the constantly evolving threats to the accuracy of age assurance methods posed by method circumvention.

Certification must be performed by an accredited third-party in accordance with ISO 17065 or an equivalent industry standard, as defined in section 700.1(a). Accreditation may be provided by the American National Standards Institute National Accreditation Board or equivalent accreditation body. Accreditation bodies that can provide ISO 17065 accreditation exist across the world.[133] The OAG proposes that certification only be performed by accredited third-parties in order to apply a uniform evaluation standard for certification and testing companies. The OAG deemed this step to be the best alternative, despite the incrementally increased burden for testing and certification companies, in order to backstop the certification

---

Enactment Impact Assessment, Oct. 23, 2024, at 61, https://www.gov.uk/government/publications/online-safety-act-enactment-impact-assessment.

[133] International Accreditation Forum, "Accreditation: A global tool to support Public Policy," *https://iaf.nu/iaf_system/uploads/documents/IAF_ILAC_B9_09_2023_English_Accred_global-tool.pdf.* For a complete list of IAF accreditation body members, *see* https://iaf.nu/en/accreditation-bodies. .

requirements in section 700.5 by ensuring that they are enforced by capable and reliable entities with the proper tools for testing and certification.

The certification process has three components: first, age assurance methods must meet the benchmarks established by ISO 27566, IEEE 2089.1, or an equivalent industry standard. The addition of an industry standard as a component of certification ensures that age assurance methods will be measured against relatively uniform benchmarks established in accordance with best practices in the industry. Allowing the option of an "equivalent industry standard" recognizes that the age assurance industry is still developing and other standards may become recognized as prevailing standards for certification and testing; these standards also may satisfy the section 700.5(a) requirement if administered in accordance with the proposed rule.

Second, the accredited third-party must determine whether the age assurance method meets the accuracy minimum. This requirement compliments the obligations in sections 700.5(b)(1) and (4), that the false positive rates of an age assurance method and the rate of detection of method circumvention be among the tests performed. Additionally, the accredited third-party must determine and report on whether the age assurance method also meets the total accuracy minimum. The OAG proposes this second requirement for certification as a method of enforcement of the accuracy minimum for all age assurance methods offered by covered operators, which is particularly important in light of the data deletion requirements in section 700.7.

The third requirement for certification of an age assurance method is the completion of the tests enumerated in section 700.5(b). Per the requirements of that section, the protocols and results of those tests must be documented, *see* 700.5(b), and the report must be maintained by the covered operator for a minimum of 10 years, *see* 700.5(d). These testing requirements beyond the application of an industry standard ensure that, regardless of the standard chosen, age assurance methods will be measured and evaluated according to specific metrics that are material to covered operators' compliance with the proposed rule.

2. Testing

The testing required by section 700.5(b) applies to any certification standard used by an accredited third-party. The testing must include the following measurable outcomes:

a. Measurement of false positive rates, false negative rates, and inconclusive age assurance outcomes

A primary objective of the proposed testing process is to document the age assurance method's accuracy rates as set forth in sections 700.5(b)(1) and (3), using the test data requirements listed in section 700.5(c). Proposed section 700.5(b)(1) requires reporting of false positive results across all data tested and such results must be broken down by age category, tracking the categories in the accuracy minimum definition. These measurements allow the

testing company to determine whether the age assurance method meets the accuracy minimum in accordance with section 700.5(b)(7).

The requirements for measurement of false negative rates track the false positive requirements except that the specified age categories are specific to the age categories listed in section 700.5(b)(3). False negative data should be used by covered operators to determine whether the age assurance method meets all obligations under applicable law, and to take all necessary actions to ensure such compliance. Covered operators should pay particular attention to discrepancies in both false positive and false negative rates to determine whether the age assurance methods offered have a disproportionately large negative effect on a basis prohibited by applicable law or otherwise treat protected groups differently.[134]

The OAG expects the rate of inconclusive age assurance outcomes, cited in proposed section 700.5(b)(2), to be used to demonstrate that at least one of the age assurance methods offered by a covered operator meets the total accuracy minimum in accordance with 700.5(b)(7). Proposed section 700.5(b)(2) also requires the collection of the reason for each inconclusive age assurance outcome, to provide transparency into how the method is functioning. This data can provide a basis for tuning the underlying age assurance method, if necessary.

b. Methods to combat method circumvention

The detection of method circumvention is a key function of any effective age assurance method. Under proposed section 700.5(b)(4), testing should be consistent with a nationally or internationally recognized testing standard, such as ISO/IEC 30107:2023 for age estimation methods. In the absence of an applicable standard for a particular age assurance method, the testing must include a variety of attack vectors and must be weighted to reflect the most prevalent method circumvention risks. The forms of method circumvention tested should mimic the type and frequency of attacks observed by the provider of the age assurance method and reported in the industry, with new types of attacks added to the testing data once they are identified as occurring in actual age assurance methods, and should reflect the level of sophistication of the age assurance method's likely users. Additionally, the volume of test data used to test and certify an age assurance method's detection of method circumvention must meet the requirements for statistical significance set forth in section 700.5(c)(1).

Method circumvention detection test results must be included in the written report documenting whether an age assurance method meets the accuracy minimum and total

[134] *See, e.g.,* Human Rights Law § 296.

accuracy minimum, *see* section 700.5(b). Additionally, the report should document the quantity and type of attack methodologies tested, in accordance with proposed section 700.5(b)(4).

c. Data handling

As detailed in proposed section 700.7(a), covered operators must adhere to specific requirements related to data minimization and deletion. As stated in proposed section 700.5(b)(5), third-party testing should include documenting the procedures implemented by the age assurance method to comply with those requirements and whether they are being followed. Additionally, the encryption and security measures used for age assurance-related data must be the subject of testing, including whether those measures meet industry standards and whether established procedures are being followed for all relevant data, per section 700.5(b)(6). To the extent a method is being administered by a third-party provider, testing of data minimization, deletion, and security measures must include data collected by the third-party provider and any data communicated between the third-party provider and the covered operator.

d. Reports, certifications, and testing data

All testing conducted in accordance with proposed section 700.5 should be documented in a written report, including both protocols and all results in accordance with section 700.5(b). Proposed section 700.5(d) states that these reports, along with all accompanying certifications and test results generated in compliance with section 700.5, should be maintained by the covered operator for a minimum of 10 years. This obligation would apply to all age assurance methods adopted by covered operators, including methods administered by third-party providers.

3. Test data

A critical element of third-party testing is the selection of data against which the age assurance method will be tested. The OAG proposes a number of specifications for this data to ensure test results for different methods and products can be trusted as fairly obtained against consistent data sets.

First, for purposes of measuring accuracy with respect to both false positive and false negative rates, the number of individual samples included in the testing data must be sufficient to ensure the reliability of the results with high confidence level and low margin of error, *see* section 700.5(c)(1). The term “high confidence” should be interpreted as a confidence interval. In addition, data subsets that reflect the respective age categories to be measured in accordance with section 700.5(b) should be represented in the overall dataset in numbers sufficient to generate reliable results for those subsets, with the same high level of confidence and low margin of error. To determine the volume of test data required for testing, the population of the State of New York most recently reported by the U.S. Census Bureau should

be used as a baseline. The OAG established these parameters to allow for a reasoned and dynamic standard to be applied to the testing process, but also to protect against test results that lack reliability due to insufficient data sets.

Second, images used as test data must reflect variations that are common in real-life photos to ensure the accuracy of the age assurance method is not too dependent upon requirements for photos that are too narrow, including conditions that may not be available to most or all users. These variations include photographic conditions, subject presentation, pose variation, and facial archetypes, all of which should be present in the test data, consistent with proposed section 700.5(c)(2).

Third, under the proposed requirements, test data, including any substantial portion of the test data, should not have been used to train or tune the age assurance product being tested under proposed section 700.5(c)(3). Using test data to train a model will skew the test results to be more favorable than they would be using new test data; this requirement protects the integrity of the testing process.

4. Certification of settings and options

Section 700.5(e) states that, to the extent an age assurance method has variable settings or options, a covered operator must only use the settings or options that received certification. The purpose of this requirement is to ensure that operators do not implement an age assurance method using alternative settings or options that, in a test environment, would not allow the age assurance method to be certified. One example of this would be turning off the "liveness" requirement that accompanies a facial age estimation check, which is an important defense against method circumvention.[135] Section 700.5(e) protects the integrity of the age assurance method's certification by requiring that the settings in the test environment match those employed with live users.

5. Alternative testing methods

The OAG encourages the use of new and innovative age assurance methods that meet the accuracy minimums but recognizes the impact of new method adoption may be that testing standards meeting the specifications in proposed section 700.5(a) are not immediately available for those methods. Where this is the case, proposed section 700.5(f) allows the covered operator to work with an accredited third-party to establish reasonable testing protocols that are consistent with the protocols listed in sections 700.5(b) and (c). The covered operator retains responsibility for ensuring the testing methods are fair and accurate. The covered

[135] Yoti White Paper, n.101 *supra*, at 14.

operator must retain records of the protocols applied to the testing and the results, to furnish upon request, for the requisite 10 years as specified in proposed section 700.5(d).

F. Section 700.6 Appeals process

1. Required framework

The proposed age assurance framework includes a mandate that covered operators create an appeals process for users who dispute being classified as minors following age assurance methods or users who refuse to provide government-issued identification for age verification. This process protects adult users from incorrect misclassification as minors and is consistent with the current state of highly effective age assurance methods, which typically have a non-zero false negative rate. The OAG recognizes that an appeals process will modestly increase the cost of age assurance methods for covered operators. At the same time, by allowing assurance methods with non-zero false negative rates, OAG is facilitating a cost-effective and healthy market for age assurance methods, which is consistent with commercial reasonability. As reflected in Part IV.B, implementation of OAG's age assurance framework, inclusive of the appeals process, remains commercially reasonable.

The framework in proposed section 700.6 affords covered operators significant latitude to create an appeals process that is compatible with their existing user flows. The process must only include "one or more methods for users to submit information and documentation in support of the appeal" under section 700.6(a)(1), and be "clear, conspicuous and accessible" to users under section 700.6(b). These requirements ensure the appeals processes designed by covered operators will serve the purpose intended by the requirement, which is access to an available method of redress for covered users who are claiming misclassification. In addition, the covered operator must provide an initial response to a covered user's appeal within 10 business days and render a final decision expeditiously upon receipt of all requested information under section 700.6(c), and that final decision must include a written summary of the appeal decision and its basis under section 700.6(a)(4). These proposed requirements would provide a uniform resolution process for covered users and protect them from undue delays.

2. Appeal decision

Under the proposed standard, the adjudication of a covered user's appeal is within the discretion of the covered operator. Proposed section 700.6(d) states that the covered operator may change an original determination of minor status based upon its review of the information submitted during the appeals process. At the same time, proposed section 700.6(a)(3) makes clear that the evidence submitted must provide a reasonable basis to reverse the covered operator's previous conclusion regarding the age status of the covered user. The OAG recognizes that many pieces of reliable evidence may rise to the level of providing a reasonable basis for reversal of the original decision. For example, a covered user could furnish a valid email address

associated with a domain available only to adults, proof of valid voter registration, or an official but non-government-issued document showing the user's age. Establishing a mechanism to evaluate and confirm the validity of this evidence is the responsibility of the covered operator with the proposed rule providing flexibility for the covered operator to determine effective methods.

G. Section 700.7 Data use and protection

1. Collection and use requirements

G.B.L. § 1501(3) requires that data collected for age assurance methods "shall not be used for any purpose other than age determination" and "shall be deleted immediately after an attempt to determine a covered user's age." Proposed section 700.7(a) reinforces and clarifies these requirements, stating that data collection should be minimized and the collected data should be used only for compliance with the proposed rule and deleted after the minimum time required for compliance, *see* section 700.7(a)(1), (2), (4).

In addition, section 700.7(a)(3) proposes requiring covered operators to use industry standard data security practices to collect and store data, including encryption of that data while it is in transit (from the covered user and, as applicable, to or from any third-party age assurance provider) and at rest (i.e., held by the covered operator or any third-party). Protection of covered user data is a primary concern. These requirements would make clear that user data may only be collected and held to the extent necessary, must be protected while it is maintained, and then must be deleted as soon as possible.

2. Maintenance of data

In light of the stringent requirements regarding data minimization and deletion of all data as a default, OAG includes a limited list of data, at proposed section 700.7(b), that covered operators must maintain to document the operation of the age assurance process. Retention of this data does not include any source data collected for age assurance methods and does not otherwise compromise the identity of covered users. Requiring that this data be maintained balances OAG's interest in confirming age assurance methods are deployed and functioning as intended with the need to protect user privacy. Retaining this data also will enable covered operators to uncover and respond to systemic problems with an age assurance method.

Additionally, proposed section 700.7(c) permits a covered operator that obtains an estimated age of a covered user to maintain that data solely for the purpose of determining age status in compliance with the proposed rule. This allows a covered operator to retain the estimated age of a covered minor, allowing the covered operator to make an informed decision as to when the covered user will reach adult age status. Obtaining an estimated age of a covered user is not mandatory.

Section 700.7(b) proposes that the data collected pursuant to the requirements of section 700.7 be retained for at least 10 years. This obligates covered operators to maintain a record of age assurance methods for future review and investigation, including by OAG as needed. Covered operators may retain the data for longer than 10 years in their discretion and in accordance with all other applicable laws.

Finally, proposed section 700.7(f) makes clear that, notwithstanding any data required or allowed to be maintained under this section, nothing in the section should be construed to require or allow use of that data to identify a user. This language is intended, for avoidance of doubt, to prohibit use of retained data to contribute to any profile or compilation of information specific to the covered user.

3. Limits of applicability

Section 700.7(d) clarifies that the requirements in the section do not apply to data collected for a purpose unrelated to compliance with the proposed rule. This provision makes clear the limits of the applicability of this section, in light of the substantial volume of data some covered operators may possess or access regarding their users for reasons unrelated to age assurance methods or related compliance.

4. Compliance with applicable law

Proposed section 700.7(e) harmonizes the requirements in the proposed rule with other current and future data protection and security laws. The proposed language states that covered operators must comply with all such laws where applicable. Where there is a conflict between the proposed rule and other applicable laws, the law that is more protective of a covered minor's privacy and safety would apply. This provision is intended to assist covered operators in navigating the landscape of data protection laws.

H. Section 700.8 Remedies

Proposed section 700.8 restates the Legislature's grant of authority under G.B.L. § 1508 to OAG to bring a special action on behalf of the State of New York in response to any perceived violation of the Act or the proposed rule. This proposed provision recognizes OAG's authority to enforce all of the requirements herein.

I. Section 700.9 Miscellaneous

Proposed section 700.9 implements the remaining provisions of the Act and other provisions necessary to effectuate and enforce it.

Proposed section 700.9(a) clarifies that all requirements apply equally to covered operators that elect to engage or otherwise rely upon any third-party. The Act imposes its

obligations on covered operators. While a covered operator may engage third-parties to assist with its compliance, it would controvert the purpose of the Act if such an engagement allowed the covered operator to evade compliance. Similarly, reliance on age signals from an app store or other third-party are at the discretion of the covered operator but responsibility for compliance remains with the covered operator regardless of the source of the age signal.

Implementing G.B.L. § 1504 of the Act, proposed section 700.9(b) states that, other than as necessary to comply with sections 700.2 and 700.3, covered operators must not: (1) withhold any product, service, or feature from a covered minor or a parent; (2) degrade or lower the quality of any product, service, or feature used by a covered minor or a parent; or (3) increase the price of any product, service, or feature used by a covered minor or a parent. Except for denying a covered minor access to an addictive feed or nighttime notifications (as dictated by a parent and a covered minor's choices), covered operators cannot discriminate against a covered minor or a parent simply because they have been identified as such or have chosen to exercise their rights under the Act. For example, a covered operator may not require a covered minor to request parental consent to an addictive feed or nighttime notifications to create a new account, nor may it require a parent to grant consent to an addictive feed or nighttime notifications for their covered minor to maintain an existing account.

A covered operator remains free to make operational decisions about its online platform, provided that the covered operator does not treat parents or covered minors differently from other users. For example, a covered operator may decide to discontinue addictive feeds for all users that it determines are below a certain age or may decide not to allow users below a certain age to continue to participate in or create an account on the platform. However, a covered operator that provides services to covered minors who obtain parental consent for an addictive feed or nighttime notification may not block covered minors who have not agreed to request parental consent, or whose parents do not consent, from accessing the same media on the platform.[136]

As another example, a covered operator may decide to charge all platform users a subscription fee to access features like notifications; however, a covered operator may not charge only covered minors a fee that other users are not required to pay. Similarly, a covered

[136] Consistent with G.B.L. § 1501(7), a covered operator is free to make independent decisions pursuant to its own policies that restrict a covered minor's access to certain media. What a covered operator may not do under G.B.L. § 1504 and the proposed rule is simply to make a decision to restrict access on the sole basis that a covered minor has the status of a covered minor. For example, if a covered minor can access a piece of media without the addictive feed (such as by searching for it or by following its creator), the covered operator may not block access to the media solely because the covered minor has declined to have a request for parental consent sent, or because the covered minor's parent has refused consent to allow the covered minor access to an addictive feed. If the covered operator independently determines that it should block the covered minor's access to the media because the media violates the covered operator's content moderation policy or other policies, it remains free to do so.

operator may not require a covered minor or their parent to upgrade their account from a free account to a paid account to access age assurance methods and verifiable parental consent options required by the Act.

Proposed section 700.9(c) states that except as expressly stated in the rule, nothing in the rule shall be construed as requiring a covered operator to give a parent any additional access to or special control over the data or accounts of a minor using an addictive online platform. This aggregates and restates G.B.L. §§ 1501(6) and 1503 as one provision for clarity. The OAG proposes minor changes to ensure that consistent defined terms are used and to clarify that the provision applies to all parents and all minors, not only to parents and covered minors who access the verifiable parental consent option. The Act does not limit other types of parental oversight of a minor's use of an online platform.

Proposed section 700.9(d) states that except as expressly and specifically required in the proposed rule or as strictly necessary to comply with applicable laws, any notice provided by a covered operator under the proposed rule shall not disclose any information to the parent that reveals a covered user's use of or other activity associated with the addictive online platform. Specifically, but not exclusively, a covered operator's notice shall not disclose: (1) personalized attributes associated with the covered minor; (2) content selections or interactions associated with the covered minor; (3) specific pieces of content that may be accessible via the addictive feed, or that may be included in nighttime notifications; (4) identities of other users of the addictive online platform; and (5) settings choices made by the covered minor. The proposed rule specifies the information required for compliance and this provision clarifies that additional information about a covered minor's use of an online platform or about other users' activity on the online platform is both unnecessary to effectuate a covered operator's obligations in this section[137] and in contravention of G.B.L. § 1503.

J. Section 700.10 Severability

Section 700.10 clarifies that all sections in the proposed rule are severable both from each other and individually. Although the proposed rule contains some cross references, the provisions of the proposed rule have been designed to work equally well separately or together, such that if any of the provisions is held invalid, the remaining provisions would continue to fulfill the purposes for which they were proposed. For example, were a court to invalidate proposed section 700.3, prohibiting nighttime notifications for minors barring parental consent,

[137] Providing unnecessary information in the mandatory notice may also confuse the parent and thus undercut their ability to grant valid consent. While a covered operator may choose to make any of this information about a covered minor available to a parent, they must do so outside of the mandatory notice.

OAG intends for the remaining provisions of the proposed rule, including proposed section 700.2 prohibiting addictive feeds to minors barring parental consent, to remain valid.

K. Section 700.11 Effective date

The OAG proposes, consistent with § 5 of Chapter 180 of the Laws of 2024, that the law go into effect on the 180th day after OAG promulgates a rule implementing the Act.

IV. Analysis of Commercial Feasibility and Costs

Under the Act, covered operators must use "commercially reasonable and technically feasible" methods to determine the user is not a covered minor. To identify commercially reasonable and technically feasible methods, the Act instructs OAG to consider several factors, including the financial and technical resources of the platform, the effectiveness of available techniques, industry practices, and user interests. As explained in Part III.D, OAG preliminarily finds a number of age assurance methods are technically feasible considering effectiveness of available techniques and user interests. The OAG conducts analyzes the commercial costs of age assurance to determine whether the technically feasible methods of age assurance discussed in Part III.D are commercially reasonable.[138]

An iterative process leads OAG to preliminarily conclude the age assurance standards in the proposed rule are commercially reasonable. Understanding the costs of effective age assurance in the current market relative to other costs faced by operators as well as the growth and monetization trajectories in the market assisted in OAG's analysis of the extent to which all covered operators can reasonably take on the costs of age assurance. Specifically, understanding the costs and the different effects of those costs on operators of different sizes or in different stages of growth led to the proposed exception for operators with fewer than 5,000,000 users globally or fewer than 20,000 users who are covered minors unless the online platform's primary user base is minors.

In assessing age assurance standards for commercial reasonability, OAG preliminarily estimates (1) the cost to covered operators of the Act's prohibition to serving addictive feeds to covered minors unless they have parental consent; (2) the cost to covered operators of implementing age assurance methods that meet the accuracy minimum for users of addictive online platforms; (3) the cost of adjusting the platform algorithms as needed to eliminate

[138] This analysis also satisfies the consideration of costs required by the State Administrative Procedures Act, or S.A.P.A. N.Y. State Admin. Proc. Act §§ 201–202. However, the analysis is overinclusive as significant economic effects estimated here are attributable to the Act itself and not to the proposed rule. For example, the prohibition on addictive feeds and nighttime notifications for minors without parental consent is mandated by G.B.L. § 1501 and the associated costs result from the Act. The OAG analyzes various costs and includes them herein to assist in promulgating these regulations and for completeness and transparency.

addictive feeds for covered minors; and (4) the economic impact of those costs for small covered operators. This Part IV also includes cost information related to parental consent.

This preliminary analysis approximates the static costs of the Act's provisions to covered operators. It does not estimate the legislation's long-run effect on overall social or economic welfare. Responses to the Act of advertisers, operators, and users will influence social and economic welfare. Likely, advertisers no longer spending funds on addictive feeds provided to minors will redirect spending to alternative uses. Operators will continue to explore other ways to monetize users' engagement and minor users will invest regained time in other activities. All these adjustments would ameliorate or offset any decrease in economic welfare that may result from the Act.[139] This analysis determines the commercial reasonability of the Act's financial burdens on covered operators and preliminarily concludes that adoption of age assurance consistent with the proposed rule would be commercially reasonable for the vast majority of operators. The OAG seeks comment on all aspects of this preliminary analysis.

The analysis relies on academic studies, industry reports, and financial documents of public firms, as well as information from operators, age assurance providers, industry and academic experts. The OAG details analytic steps and assumptions, including structural assumptions, of the preliminary analysis and welcomes comment on every aspect of the analysis and results. The OAG also requests additional relevant data including about addictive online platforms and their users and about the age assurance industry.

For ease of reference, this preliminary analysis refers to the requirement that operators conduct age assurance on covered users to determine whether they are covered minors as the "SAFE age assurance requirement." It refers to the prohibition in section 700.2 on using information persistently associated with a covered minor or covered minor's device or the user's previous interactions with user generated media without parental consent as the "SAFE personalized feed ban."

As an upper bound to effects on revenue from the SAFE personalized feed ban, OAG does not reduce the revenue impact based on anticipated parental consent to a minor receiving a personalized feed. Addictive online platforms get all or a significant portion of their revenue from user engagement, generally through targeted advertising, and thus, revenue will be less impacted if minors receive parental consent and continue receiving addictive feeds. With no definitive data to support an assumption as to what percent of parents would consent, the analysis conservatively assumes no parents will consent as an upper bound for estimating potential revenue loss.

---

[139] This analysis does not quantify such adjustments because doing so is uncertain and inherently speculative. It would require copious data, which is not available currently.

A. Cost of SAFE Personalized Feed Ban

The preliminary analysis first models the costs to operators of the SAFE personalized feed ban. The analysis predicts a decrease in covered operators' revenues through two main pathways. First, OAG assumes the SAFE personalized feed ban will reduce the addictiveness of feeds provided to minors by covered operators. A decrease in feed addictiveness is likely to diminish the time minors spend on addictive online platforms, leaving covered operators with fewer user-minutes to monetize through advertising.[140] Second, an inability to plant targeted advertisements in minors' feeds is likely to decrease the price at which covered operators can auction the opportunity to advertise to their underage users.[141] The Act also may impact other revenue streams, but as discussed below, data on those streams is scarce and any changes are likely negligible in comparison to those mentioned above.

The market for social media platforms is relatively concentrated.[142] This analysis focuses on six of the largest such platforms as the starting point because greater information is publicly available on their finances and algorithms. Most importantly, available data detailing the revenue of social media platforms attributable to minors focuses only on six platforms.[143] These generally well-known "Big Six" social media platforms are: Facebook, Instagram, YouTube, TikTok, Snapchat, and Twitter/X.

This analysis extrapolates from the Big Six to industry-wide estimates, which is possible because of the concentration in the social media market and the current business model for

---

[140] Andrew Guess, *et al*., *How do social media feed algorithms affect attitudes and behavior in an election campaign*, Science, Vol 381, Issue 6656, 27 Jul 202, pp. 398-404, doi: 10.1126/science.abp9364.

[141] The Act does not categorically ban targeted advertising or otherwise focus on advertising or advertisers. Instead, it generally prevents covered operators from personalizing the user-generated media a covered minor receives. On most covered operators' platforms, advertisers' sponsored content is promoted within users' feeds as if it were any other post. Insofar as advertising on platforms occurs within feeds (and, as discussed herein, much or all of it does) it may not be served to minors if its delivery hinges on the user's data or metadata. Put simply, covered operators are barred from showing targeted, in-feed ads to minors.

[142] Alissa Cooper and Zander Arnao, *Concentration in Social Media Undermines Product Design Quality and User Experience*, Promarket, Mar. 4, 2025, https://www.promarket.org/2025/03/04/concentration-in-social-media-undermines-product-design-quality-and-user-experience. The Act generally defines covered operators based on their use of addictive feeds for user-generated media as a feature that is a substantial part of their services, and thus, may cover online platforms that would not be colloquially referred to as social media. This analysis examines the social media industry as a proxy for covered operators, given both the likelihood of social media platforms being covered and the heavy reliance of social media platforms on user engagement to generate revenue.

[143] Amanda Raffoul, *et al.*, *Social media platforms generate billions of dollars in revenue from U.S. youth: findings from a simulated revenue model*, PLoS One, Dec. 27, 2023, doi: 10.1371/journal.pone.0295337, https://pubmed.ncbi.nlm.nih.gov/38150418/.

generating revenue, which is typically through advertising. The analysis also takes into account the current policies of the Big Six with respect to limiting their services to certain age groups and limiting or prohibiting targeted advertising to minors. As of the date of publication four of the Big Six state publicly that they have stopped allowing targeted advertising to minors.[144] The OAG seeks comment and data on the market for addictive online platforms, revenue, sources of revenue, revenue attributable to minors, and other aspects of this preliminary analysis.

1. Advertising revenue lost from diminished time spent by minors

This analysis first estimates the Act's predicted effect of a decrease in monetizable user time by minors. One result of the Act will be that minors in New York will spend less time on addictive online platforms. The analysis, thus, examines the impact of reduced user time on revenue, based in part on whether the platforms currently direct targeted ads to minors.

For each of the Big Six, Table 1 displays the platform's 2024 revenue, the portion of that revenue earned through advertising, and the portion of that ad revenue earned in the United States.

[144] These decisions were implemented generally between 2022 and July of 2025. *See* Facebook, "Announcing Changes to the Ways Teens Can be Reached on Facebook and Instagram," Jan. 10, 2023, https://www.facebook.com/government-nonprofits/blog/evolving-how-advertisers-reach-teens-on-our-platform ("Advertisers will only be able to target teens based on age and city-level or greater location (e.g. state). We will remove the ability to target teens by gender or any location more granular than city (e.g. zip code); this follows last year's targeting updates, which included removing the ability to target teens by detailed targeting options (e.g. interest) or Custom Audiences (e.g., customer list)."); Instagram, "How ads are different for teens," https://privacycenter.instagram.com/dialog/how-ads-are-different-for-teens (to users under 18: "Businesses can only decide to include you in an audience based on your age and location to show you ads that you may like."); Mindy Brooks, "Giving kids and teens a safer experience online," Google, Aug. 10, 2021, https://blog.google/technology/families/giving-kids-and-teens-safer-experience-online ("The Ad-serving protections for children policy applies on YouTube, Google Display Ads, and Display & Video 360 campaigns, and additional products will be added over time. These protections include disabling ads personalization . . . ."); TikTok, "Enhancing privacy and control: new ad experience and tools for TikTok users and advertisers," July 3, 2024, https://ads.tiktok.com/business/en-US/blog/enhancing-privacy-control-advertisers-users ("Starting June 30, [2025] we are adding further restrictions to advertising to teens. Advertisers will not be able to reach teens in the United States using any personalized targeting and campaign selections. Advertisers will only be able to reach teens using a few broad targeting options, such as location, language, and device-related information.").

Both SnapChat and Twitter/X presumably continue to allow ad targeting to minors 13 to 17 years old.

Table 1: Big Six Revenue[145]

	Total Revenue 2024 (billions)	% Ad Revenue	% US Ad Revenue
Facebook	$93.0	98%	42%
Instagram	$66.9	100%	69%
Twitter/X	$2.5	68%	58%
Youtube	$54.2	67%	23%
TikTok	$23.0	77%	59%
Snapchat	$5.4	91%	60%

[145] The following sources were used for revenue estimates:

Instagram: Nayden Tafradzhiyski, *Instagram Revenue and Usage Statistics (2025)*, Business of Apps, https://www.businessofapps.com/data/instagram-statistics; Ellen Simon, *How Instagram Makes Money*, Investopedia, June 16, 2024, https://www.investopedia.com/articles/personal-finance/030915/how-instagram-makes-money.asp; Albert Mosby, *Instagram Ad Revenue From 2018-2025 (Demographics)*, Yaguara.co, Jan. 2, 2025, https://www.yaguara.co/instagram-ad-revenue

Twitter/X: Nayden Tafradzhiyski, *Twitter Revenue and Usage Statistics (2025)*, Business of Apps, https://www.businessofapps.com/data/twitter-statistics; Jaspreet Singh, *X to report first annual ad revenue growth since Musk's takeover, data shows*, Reuters, March 26, 2025, https://www.reuters.com/technology/x-report-first-annual-ad-revenue-growth-since-musks-takeover-data-shows-2025-03-26/

YouTube: Nayden Tafradzhiyski, *YouTube Revenue and Usage Statistics (2025)*, Business of Apps, https://www.businessofapps.com/data/youtube-statistics; Sara Lebow, *5 charts that demonstrate YouTube's reach: Ad spend, users, and Gen Z*, Emarketer, Jul. 29, 2024, https://www.emarketer.com/content/5-charts-that-demonstrate-youtube-s-reach-ad-spend-users-gen-z

TikTok: Nayden Tafradzhiyski, *Tik Tok Revenue and Usage Statistics (2025)*, Business of Apps, https://www.businessofapps.com/data/tik-tok-statistics; Daniel Ruby, *TikTok Ad Revenue (2020-2027) - Detailed Analysis*, Demandsage, Sept. 6, 2025, TikTok Ad Revenue (2020–2027) – Detailed Analysis

Facebook: David Curry, *Social App Report 2025*, Business of Apps, https://www.businessofapps.com/data/social-app-report; Meta Platforms, Inc., Annual Report (Form 10-K), Jan. 29, 2025, https://www.sec.gov/Archives/edgar/data/1326801/000132680125000017/meta-20241231.htm; Jessica Deyo, *Facebook global ad revenue to surpass $100B in 2024: WARC*, Yahoo Finance, Dec. 12, 2024, https://finance.yahoo.com/news/facebook-global-ad-revenue-surpass-090800146.html

Snapchat: Nayden Tafradzhiyski, *Snapchat Revenue and Usage Statistics (2025)*, Business of Apps, https://www.businessofapps.com/data/snapchat-statistics; Krystal Scanlon, *Ad revenue or subscriptions: What's more viable to Snap's success as a business?*, Digiday, Dec. 25, 2024, https://digiday.com/marketing/ad-revenue-or-subscriptions-whats-more-viable-to-snaps-success-as-a-business; Snap, Inc., Annual Report (Form 10-K), Feb. 4, 2025, https://www.sec.gov/Archives/edgar/data/1564408/000156440825000019/snap-20241231.htm

Note: "Total Revenue (2024)" shows the global gross revenue measured in USD; "% Ad Revenue" shows the percentage of that revenue derived from advertising; "% US Ad Revenue" shows the percentage of platform ad revenue earned from advertising to U.S. users.

First, to estimate the total ad revenue for each platform in New York, the three amounts are multiplied by each other, as well as the portion of U.S. social media users who reside in New York, which is 5.72% based on the portion of the U.S. population in New York.[146] The next step involves two parameters: the portion of ad revenue on each platform derived from minors and the decrease in user engagement that follows an exogenous switch from an algorithmic to a chronological feed. A collection of academic research papers jointly provides these parameters, which are displayed in Table 2.[147] For Snapchat, no high-quality estimates of a predicted decrease in user engagement exist. As algorithmic feeds represent a smaller portion of its service than for the rest of the Big Six, the analysis applies the estimated upper bound of 0.13 or 13% (a decrease equal to that of Instagram). For the rest of the platforms, the estimates are assumed to be the same as estimates in the related research.

---

[146] To calculate the U.S. social media users who reside in New York, the analysis assumes social media users are distributed across the U.S. consistent with the distribution of the population generally. Accordingly, the analysis calculates New York's percentage of social media users by dividing the population of New York by the U.S. population. Based on 2024 Census Data this is equal to 19,867,248/347,279,000 = 5.72%.

[147] The estimated decrease in engagement comes from multiple papers. Guess *et al.*, n.140 *supra*, reports decrease in user engagement in Facebook and Instagram. For Twitter, the estimate relies on Gauthier, *et al*., "The Political Effects of X's Recommender Algorithm," Working Paper (2025). For Tik Tok, the estimate relies on Aarushi Kalra, *Hate in the Time of Algorithms: Evidence on Online Behavior from a Large-Scale Experiment*, General Economics, Mar. 8, 2025, https://doi.org/10.48550/arXiv.2503.06244, which studies a short-form video platform in India with a similar user interface to TikTok. For YouTube, no directly analogous study is available; the estimate represents the midpoint between Twitter and TikTok.

The percentage of ad revenue attributable to minors is taken from Raffoul *et al*., n.143 *supra*. Because it measures revenue rather than engagement, it accounts for the time minors spend on platforms in addition to platforms' ability to monetize that time. It does not, however, take into account the reduction in the value of user minutes resulting from some platforms' decision to cease targeted ads for minors. That reduction is addressed in subsequent paragraphs.

There are two important points to note about these engagement decrease estimates. First, the studies above measure engagement decreases when feed changes are implemented on a single platform and users could substitute to other platforms. As the SAFE for Kids Act regulates the provision of any algorithmic feed to minors across platforms, engagement decreases that represent diversion to other platforms may be smaller than previously estimated. Therefore, the engagement decrease estimates above likely overestimate the true effects of the Act. Second, research shows that many users report that they think they are using social media too much. *See* Hunt Allcott, *et al.*, *Digital Addiction*, American Economic Review, July 2022, doi: 10.1257/aer.20210867. For that reason, a decrease in engagement may actually increase consumer welfare.

Table 2: Big Six Revenue from Minors & Expected Engagement Decrease

	Est. Engagement Decrease	Ad Revenue from Minors
Facebook	26%	2%
Instagram	13%	17%
Twitter/X	14%	2%
YouTube	20%	27%
TikTok	28%	36%
Snapchat	13%	42%

"Est. Engagement Decrease" shows for each platform the estimate of the engagement decrease that will likely result from the proscription against providing algorithmic feeds to minors. "Portion of Ad Revenue from Minors" shows the percentage of platform ad revenue derived from advertising to minors.

To approximate the reduction in advertising revenue for each platform, the total New York advertising revenue for each platform is multiplied by the portion of ad revenue attributable to minors and the engagement decrease resulting from the removal of an algorithmic feed.

$$\Delta \text{ ad rev}_{safe} = \text{ad rev}_{SQ} * \% \text{ ad rev}_{minors\ SQ} * \text{expected \% engagement decrease}$$

Next, the analysis accounts for the change in four of the platforms' policy decision to stop targeted advertising for minors as described above. The estimate of percentage of ad revenue from minors was derived before those changes occurred—i.e., when the four platforms were still targeting advertising for minors. Thus, the analysis reduces the percentage of overall advertising revenue attributable to advertisements directed to minors because platforms generally price non-targeted advertising lower than targeted advertising. Specifically, the change in revenue for the four platforms that no longer target to minors is discounted by the difference in price for targeted versus non-targeted advertising. The first step in evaluating the discount to apply to this revenue stream is ascertaining the volume of advertisements that are both in-feed and targeted on the Big Six platforms.

Approximately 92% of advertisers on the largest social media platforms utilize targeting and virtually all of this advertising occurs within feeds.[148] Accordingly, the 8% of revenue not attributable to targeted advertising should not be discounted. The analysis thus estimates that

[148] Manisha Saini, "40+ Targeted Advertising Statistics: Data-Driven Marketing Insights [2025]," Cropink, last updated Mar. 31, 2025, https://cropink.com/targeted-advertising-statistics; Reuters, *Instagram to make up more than half of Meta's US ad revenue in 2025, report shows*, Dec. 18, 2024, https://www.reuters.com/technology/instagram-make-up-more-than-half-metas-us-ad-revenue-2025-report-shows-2024-12-18/.

the value of 92% of revenue from advertising to minors for the four platforms that ended targeted advertising for minors must be discounted.

To calculate the value by which that reduction in revenue is discounted, the analysis next estimates how much the value of that advertising will decrease. Public empirical evidence on the difference in price that advertisers pay for targeted vs. contextual advertising is scant, but one study estimates that advertisers pay roughly 45% more for targeted advertising.[149] These parameters imply that covered operators' advertising revenue to minors can be valued at 0.71 of the revenue estimated for targeted advertising for the four non-targeting platforms before dynamic adjustments.[150] Accordingly, for the four non-targeting platforms, the outputs from the formula above are further multiplied by .71.

Δ ad rev_{safe} = ad rev_{SQ} * % ad $rev_{minors\ SQ}$ * expected % engagement decrease * discount in price paid for non-targeted advertising, pre-regulation

The product is the estimated ad revenue loss for each of the Big Six platforms due to the Act's prohibition on serving algorithmic feeds to minors in New York.[151] These calculations are displayed in Table 3.

[Space intentionally left blank]

[149] Ayman Farahat, *et al.*, *How effective is targeted advertising?*, WWW '12, Proceedings of the 21st international conference on World Wide Web, April 2012, pp.111-120, https://doi.org/10.1145/2187836.2187852.

[150] The portion of advertising that will decrease in revenue (0.92) is multiplied by the decrease (1/1.45), and the product is then added to the portion of advertising that will not decrease in revenue (0.08). The sum is the ratio of the value of minor-directed advertising for non-targeted advertising (and before dynamic adjustments) versus targeted advertising.

[151] This portion of our analysis assumes that the price of auctioning the opportunity to advertise is unaffected by quantity sold. In fact, advertisers are likely to be willing to pay more per unit for the first minute of advertising than the ten millionth (as demand curves slope downwards), so this is likely an overestimate of revenue loss from engagement decrease.

Table 3: Estimated NY Ad Revenue & Projected Loss Based on Reduction in Time Spent on Platform by Minors from the SAFE for Kids Act

	NY Ad Revenue	Discount Based on Non-Targeting?	Total Revenue Reduction
Facebook	$2.2 billion	Yes	$ 8 million
Instagram	$2.6 billion	Yes	$41 million
Twitter/X	$56 million	No	$158,000
Youtube	$478 million	Yes	$18 million
TikTok	$598 million	Yes	$43 million
Snapchat	$167 million	No	$9 million
Total (Big Six)	**$ 6.1 billion**		**$119 million**

"NY Ad Revenue" shows the estimated advertising revenue for each platform in the State of New York. "Discount Based on Non-Targeting?" indicates whether the reduction in revenue was discounted to account for the platform's previous decision to ended targeted advertising to minors."Total Revenue Reduction" shows the projected decrease in that NY ad revenue as a result of the likely drop in user engagement.

The estimated total revenue loss for all firms is approximately 1.9% of their New York advertising revenue and 0.05% of their U.S. advertising revenue.

To calculate an industry-wide estimate of change in advertising revenue for all covered operators or the market of social media platforms, OAG relies on a series of calculations to extrapolate. The estimate of revenue for the Big Six together with an estimate of total advertising spend in the market is used to calculate the market share of that advertising spend attributable to the Big Six.[152] The Big Six ad revenue loss is divided by their market share (95%)

[152] Estimating digital advertising spend across the market is tricky, as the SAFE for Kids Act covers a bespoke aggregation of platforms broader than the colloquial term "social media", but narrower than the entire digital advertising market for display and video. Because the true market comprises not just large social media platforms but also countless small and mid-sized platforms, simply summing platforms' ad revenue is infeasible.

to receive an estimate of ad revenue loss for all covered operators. So, while the Big Six estimates serve as a baseline for modeling the portion of ad revenue lost by covered operators, the final estimate of ad revenue loss accounts for all covered operators regardless of scale. In conclusion, the ad revenue lost by all covered operators due to the Act's proscription against offering algorithmic feeds to minors is likely approximately $126 million.

2. Advertising revenue lost from decreased minor user-minute value

The second pathway through which the SAFE for Kids Act's provisions may decrease covered operators' ad revenue is an inability to deliver targeted, in-feed advertising to minors that diminishes the price at which covered operators can auction the opportunity to advertise to underage users. The Act does not categorically prohibit targeted advertising to minors but it does prevent covered operators from algorithmically recommending or sorting content within minors' feeds on the basis of personal data or metadata without parental consent.

For the four non-targeting platforms, the reduction in the user-minute value is discounted to zero. The Act's prohibition on targeted advertising will capture targeted ads that those four platforms are currently serving to minors because those minors are incorrectly passing as adults—and almost none will continue to be able to do so after age verification consistent with the Act is in place. This estimate, however, does not account for targeting revenue operators might gain from those minors because first, they do not intend to earn that revenue and second, the targeting is likely ineffective and overall reducing the value of targeted ads because it is based on inaccurate information about the individual being targeted.

Again, the following analysis is static in nature and thus necessarily limited, especially with respect to this revenue stream. Advertisers and platforms will innovate to retain the value of the attention of minors they continue to have and likely find ways to maximize contextual advertising or to increase prices for contextual advertising that will have a more reliable audience of minors. For the two platforms with advertising targeted to minors, the lost value parameter (1-0.71) is multiplied by the total NY ad revenue associated with minors that remains

---

Instead, the analysis uses a simple average of ad spend in the too-narrowly defined social media market and the too-broadly defined display and video market.

See iab.com, pwc.com, e&m: "Internet Advertising Revenue Report, Full-year 2024 results," April 2025, https://www.iab.com/wp-content/uploads/2025/04/IAB_PwC-Internet-Ad-Revenue-Report-Full-Year-2024.pdf (88,800,000,000 + 136,400,000,000)/2 = 112,600,000,000.) This is an imprecise estimate. However, the 95% market share it implies for the Big Six does accord roughly with independent estimates. Additionally, because this approach assumes that monetization of minor users does not vary with platform size (when, in fact, larger platforms are much more effective at monetizing user-minutes), it is likely an overestimate of lost revenue.

after the decrease in minors' engagement predicted in Part IV.A(a). The product is lost ad revenue. The results of these calculations are displayed below in Table 4.

Table 4: Ad Revenue Loss for Loss of Targeted Advertising to NY Minors

	Revenue Loss for Loss of Targeted Ads
Facebook	$0
Instagram	$0
Twitter/X	$283,000
Youtube	$0
TikTok	$0
Snapchat	$17.6 million
Total (Big Six)	**$17.9 million**

"Ad Revenue Loss " shows the loss to the estimate of remaining NY minor ad revenue due to restrictions on targeted advertising. .

From these totals, dividing the relevant market share, as in (a), provides the industry-wide estimates of ad revenue lost to the Act's proscription against targeted, in-feed advertising to minors. In conclusion, the total industry-wide advertising revenue lost through this pathway is approximately $17.9 million.

3. Results

The total advertising revenue lost by covered operators due to the Act's provisions (before the cost of compliance with age assurance requirements), calculated by summing the estimated diminution in the two revenue streams identified above, is thus approximately $144 million. No other significant source of revenue is likely to be substantially affected as a result of the Act's prohibition on serving algorithmically curated feeds to minors.[153] This range is therefore a reasonable estimate of the static cost of the Act to covered operators.

However, again, the true dynamic or long-run cost to covered operators is likely to be lower, as operators will adjust to the Act's provisions and some parents will consent for their minor children to receive addictive feeds.

[153] Although attempted, an estimate of the non-ad revenue platforms might lose due to lower minor engagement was not feasible. Non-ad revenue makes up a small to miniscule portion of the Big Six platforms' revenues, and it usually takes the form of subscription sales or shops embedded in the platform. There is scant data on these other revenue streams, and what data does exist indicates that the likely decrease in revenue would be negligible. These other revenue streams likely do not decrease monotonically with minors' user engagement decreases as does ad revenue, and it is likely that minors account for a lower portion of other revenues (subscriptions, store purchases) than ad revenues.

Table 5 displays these composite lost revenue statistics. It also presents this lost revenue divided by the number of NY minors protected by the ban on algorithmic social media feeds (in other words, minors that would likely be served addictive feeds if not for the SAFE for Kids Act).[154] The resulting number can be thought of as one representation of the combined "cost" to addictive social media platforms of protecting one minor from the harms of addictive feeds. And, of course, the academic literature supports a high estimate of the benefits of protecting one minor from the harms of addictive feeds, including a reduction in digital addiction, improvement in well-being, and increase in other activities.[155] The benefits are inherently intangible, but when the New York legislature passed the Act, it determined that the value of such benefits is significant.

Table 5: Aggregate Ad Revenue Decreases

	Decrease in Engagement	**Decrease in Engagement & Targeting**
Total Revenue Loss	$126 million	$144 million
NY Minors Protected	1,509,775	1,509,775
Revenue Loss Per Minor	$84	$95

"Decrease In Engagement" refers only to ad revenue lost from diminished engagement as a result of the Act's proscription against algorithmic feeds. "Decrease in Engagement & Targeting" refers to the aggregate ad revenue lost "NY Minors Protected" is the estimated number of NY Minors who will not be served algorithmic feeds as a result of the Act. The next row shows the industry-wide revenue loss per NY minor protected).

In conclusion, the analysis indicates that the Act's provisions will cost covered operators at most $144 million in annual revenue. This translates to approximately $95 across all covered platforms in foregone annual revenue per NY minor protected from addictive feeds.

B. Cost of SAFE Age Assurance Requirement

The previous section analyzed the cost of the Act to covered operators without taking into account age assurance adoption and maintenance costs. This section estimates the costs of the SAFE age assurance requirement for platforms of various sizes. Specifically, the costs are assessed for platforms of five different sizes: Our hypothetical platforms 1-5 respectively, have

[154] The number of NY minors likely to be affected by the Act was calculated by first finding the number of NY children ages 8-12 and 13-18 using U.S. Census data. Then, rough estimates of the portion of minors in both age bands who use social media were utilized: 40% and 95%. *See* U.S. Surgeon Gen., Advisory, *Social Media and Youth Mental Health*, at 4 (2023). These numbers are for social media traditionally defined and likely underestimate the number of minors affected by the Act's provisions.

[155] *See, e.g.*, B. Keles, *et al.*, *A Systematic Review: The Influence of Social Media on Depression, Anxiety and Psychological Distress in Adolescents*, International Journal of Adolescence and Youth, 25, 79-93 (2019), https://doi.org/10.1080/02673843.2019.1590851.

global monthly average users of 900,000,000; 100,000,000; 20,000,000; 2,000,000; and 500,000.

1. Platform financials

For each platform type, estimated parameters include annual revenue, total costs and expenses, annual user growth, and various wage rates. These values are not necessarily averages across all platforms in a particular size range; they are instead an attempt to plausibly simulate the financials of a covered operator's platform of a certain size.

The preliminary analysis begins with estimated data on monthly average users (MAU) and revenue from 11 platforms of various sizes that feature user-generated content.[156] From this data the analysis extracts average revenue per user values for different platform sizes. This is not a precise revenue per user (RPU) number like that platforms often use to capture the value of revenue flows linked to an individual user; rather it assists in predicting a firm's income statement revenue from its monthly user base.

Next, for the three platforms in the previous group that are public, and thus publish cost data, the analysis divides platform revenue by total costs and expenses and averages these three results. This results in an average ratio of revenue to costs of 0.689.[157] These two parameters (RPU and revenue-to-cost ratio) along with data on small and very small platforms from a SaaS tech startup survey are used to estimate the financials for the five platform types. The analysis also inputs a parameter for U.S. MAU linked to global MAU.[158]

[Space intentionally left blank]

[156] These platforms are: Nextdoor, Eventbrite, Indeed, Pinterest, Reddit, LetterBoxd, Substack, Rumble, Beli, Fishbowl, and Pepper.

[157] These three platforms were: Nextdoor, EventBrite, and Rumble.

[158] The MAU numbers for platform 1 are based on Snapchat's reported MAU estimates. *See* n.145 *supra.* For platform 2, a scalar (between US and global MAU) of 4 is used, similar to many platforms of similar sizes (*e.g.*, Pinterest or Rumble). For the smaller platforms, the analysis steadily decreased this scalar to produce the largest and thus most conservative estimate of age assurance costs for small platforms.

Table 6: Platform Financials[159]

Other Info	Platform 1	Platform 2	Platform 3	Platform 4	Platform 5
US MAU	110,000,000	25,000,000	6,666,667	1,000,000	300,000
Global MAU	900,000,000	100,000,000	20,000,000	2,000,000	500,000
Costs & Exp.	$6.15 billion	$465 million	$35 million	$2.5 million	$0.7 million
Revenue	$5.36 billion	$320 million	$24 million	$360,000	$89,000
US User Turnover	15,000,000	4,333,333	3,911,111	1,000,000	300,000

"U.S. MAU" shows the number of monthly average users for each type of platform in the U.S. "Global MAU" shows the same internationally. "Costs & Exp." shows the aggregate costs of goods sold plus all other annual expenses incurred. "Revenue" shows annual revenue. "User Turnover" shows the number of new U.S. users annually for which platforms must perform age assurance.

Next, several wages and expense types are estimated for each platform type, displayed below in Table 7. Again, these are not strict averages for such platforms but an illustrative example of such expenses.

[Space intentionally left blank]

---

[159] The values for platform 1, the "large platform," are those of Snapchat. See n.145, *supra*.

For platform 2, MAU is multiplied by RPU to estimate revenue, as for all platform types below. Revenue is divided by the revenue-to-cost ratio to find costs and expenses. The annual user growth value comes from Nextdoor's annual user growth in 2023 from 75 million to 88 million. *See* Business Wire, *Nextdoor Reports Fourth Quarter and Full Year 2023 Results*, Feb. 27, 2024, https://www.businesswire.com/news/home/20240227020537/en/Nextdoor-Reports-Fourth-Quarter-and-Full-Year-2023-Results.

For platform 3, OAG obtained the costs and expenses value using the same formula as for platform 2. The user growth rate was a simple average of that for platform 2 and for platform 4, which is explained below.

For platform 4, the costs and expense value was obtained by adding $2.1 million to platform revenue. *See* 2022 SaaS Benchmarks Report, OpenView Partners, at 13, https://openviewpartners.com/2022-saas-benchmarks-report/#ch5. The user growth rate was set at 100%, *see id*.

For platform 5, the cost estimate was obtained as above, this time with the average monthly burn rate of $50,000. User growth is also obtained as for platform 4.

Table 7: Platform Wages & Expenses[160]

	Platform 1	Platform 2	Platform 3	Platform 4	Platform 5
Software Engineer	$130	$100	$70	$54	$50
Legal	$1,000	$500	$350	$250	$200
Business	$100	$80	$60	$50	$40
Customer Service	$25	$25	$25	$25	$25

The rows display the hourly wage for each occupation: software engineers, lawyers, business development, and customer service.

2. Age assurance cost information

The preliminary analysis next estimates the cost of age checks. This analysis assumes a simple waterfall age assurance setup as described in Part III.D, where the platform contracts with a third-party provider to screen users through biometric facial age estimation and, if facial

[160] The OAG estimates that relative to the size of the platform, the operator will engage more or less costly assistance, based in part on relative revenue and potential complexity associated with larger platforms and businesses generally. Estimates for legal wages are based on OAG's expertise and a variety of sources of data reported. *See, e.g.,* Brightflag, *Hourly Rates in Am Law 100 Firms: Increases and Key Drivers*, 2024, https://brightflag.com/asset/law-firm-rates-report/?; Catherine Brock, *How much is a Lawyer? Hourly Rates by State and More*, Nov. 12, 2024, https://www.lawpay.com/about/blog/lawyer-hourly-rate-by-state/. As noted in the analysis of costs related to parental consent, the FTC estimates hourly legal costs for implementation of changes to COPPA based on the Fitzpatrick Matrix, which estimates rates for complex federal litigation in the District of Columbia, resulting in a weighted rate for associate and partner time of $655 per hour. COPPA Rule, 90 Fed. Reg. 16918, 16974 n. 684 (April 22, 2025). The U.S. Bureau of Labor Statistics reports median lawyer wages in New York to be $85.20 per hour and in D.C. to be $92.25 per hour. *Occupational Employment and Wage Statistics - Research estimates by state and industry*, May 2024, https://www.bls.gov/oes/tables.htm. While the median per hour salaries are similar between New York and D.C., they are significantly lower than the Fitzpatrick Matrix cited in the COPPA Rule. The OAG uses a higher scale to reflect an upper bound of legal costs. For software engineers, business development, and customer service, OAG similarly uses multiple sources of data together with its expertise to estimate a range of wages. For software engineers, *see, e.g.*, Levels.fyi, *Snap Software Engineer Salaries*, Sept. 14, 2025, https://www.levels.fyi/companies/snap/salaries/software-engineer?country=254; Inna Coker, *Guide to Software Engineer Salary in US: Rates Comparison by State in 2025*, Feb. 27, 2025, https://qubit-labs.com/software-engineer-salary-in-usa/. For business development, *see,* e.g., Levels.fyi, *Snap Business Development Salaries*, Sept. 14, 2025, https://www.levels.fyi/companies/snap/salaries/business-development; Indeed, *Business development manager salary in United States,* Sept. 8, 2025, https://www.indeed.com/career/business-development-manager/salaries). For customer service, *see, e.g.,* Wow24-7, *How Much Does It Cost to Outsource Customer Service?*, Sept. 8, 2025, https://wow24-7.com/blog/how-much-do-different-call-centers-cost-for-outsourcing-call-center-outsourcing-cost-comparison-2.

age estimation fails or is bypassed, document verification.[161] The analysis also accounts for the appeal process mandated in the proposed rule. The cost estimates are displayed in Table 8.

Table 8: Age Check Costs Per User

(Per User)	**Cost (1)**	**Cost (2)**	**Cost (3)**	**Cost (4)**	**Cost (5)**
Biometric Scan	$0.05	$0.10	$0.13	$0.15	$0.15
Document Verification	$0.08	$0.10	$0.10	$0.10	$0.15
Appeal	$6.25	$6.25	$6.25	$6.25	$6.25

The rows display the marginal cost of performing each level of age assurance for a single user. The columns display the per user cost for each platform type 1-5. The decreasing costs with scale indicate bulk discounts offered by age assurance providers.

The cost estimates for facial age estimation and document verification come from public documents provided by age assurance providers. The cost for document verification indicates the marginal cost of escalating to document verification if the facial age estimation fails or is bypassed.[162] The cost for appeal is estimated by multiplying the estimated time required for an appeal by the prevailing customer service wage shown above.[163] Another parameter necessary for these calculations is the percentage of customers successfully assured at each step in the waterfall. This data, also shared publicly by entities in the age assurance industry, is displayed below in Table 9. Successful in this case does not necessarily mean accurate

Table 9: Age Check Success

	% Successfully Assured
Facial Age Estimation	82%
Document Verification	97%
Appeal	100%

The rows display the percentage of users successfully assured by each level of age assurance.

---

[161] There may be many age assurance techniques that can reach accuracy minimums set out in the proposed rule, but information reviewed by OAG shows that such methods tend to be no more expensive than these two. *See, e.g.*, *Free Speech Coalition v. Paxton*, No. 23-1122, Br. of *Amicus Curiae* Age Verification Providers Assoc'n, at 19 (Nov. 2024) ("An adult site can typically complete age checks with AVPA members for approximately 12 cents per user per year, and this cost is expected to fall as age-verification technology continue to advance.").

[162] Pricing models in the age assurance industry differ with respect to circumstance. Some pricing models do not charge extra if a user must be escalated to a higher level of age assurance but charge more up front for access to those higher levels. This variation in the pricing model has no effect on the calculations above.

[163] The OAG estimates that the appeal process set out in the proposed rule will use up roughly 15 minutes of customer service time per user, so the cost is calculated by (1/4) times the hourly customer service wage.

Next, for each platform type, the fixed costs of adapting a platform to incorporate age assurance for all users are estimated. These cost estimates, expressed in terms of wage-hours, were based on information from industry experts, and they are displayed in Table 10.

Table 10: Fixed Compliance Costs

	Hours (5)	Hours (4)	Hours (3)	Hours (2)	Hours (1)
Project scoping & vendor selection	40	60	90	120	200
Technical integration: new users	35	50	75	105	210
Retroactive application: old users	105	130	225	315	630
User testing and iteration	40	50	60	70	120

The rows display the hours necessary to complete four discrete tasks that together represent the process of constructing an age assurance apparatus in accordance with the Act.

The same analysis is conducted for annual, recurring compliance costs introduced by the Act's age assurance requirements. Recurring costs are displayed below in Table 11.

Table 11: Annual Compliance Costs

	Hours (5)	**Hours (4)**	**Hours (3)**	**Hours (2)**	**Hours (1)**
Legal Hours	40	50	100	150	200
SWE Hours	80	140	170	200	480

The rows display the necessary annual labor expressed in terms of hours from both lawyers and software engineers to maintain an age assurance apparatus in accordance with the Act.

Finally, the analysis includes the cost of adjusting the platform's algorithms so that an addictive feed is no longer delivered to covered minors. These estimates are also based on expertise and industry input. This cost category does not include any features that platforms choose to change or add to enhance the user experience for covered minors following the cessation of personalized feeds; such costs are not required and will vary by platform so are not possible to calculate.

Table 12: Algorithm Adjustment Costs

	Hours (5)	**Hours (4)**	**Hours (3)**	**Hours (2)**	**Hours (1)**
Project scoping	40	50	90	120	240
Technical execution & testing	80	100	180	240	480

The rows display the number of hours necessary for software engineers to adjust platform algorithms for covered minors in accordance with the Act. "Project scoping" refers to the planning phase of algorithm adjustment, including cross-functional collaboration with the compliance and product functions. "Technical execution & testing" refers to the work performed and tested by engineers.

3. Results: Age assurance costs

The inputs in Parts IV.B.1 and 2 are used to estimate the fixed and recurring costs of age assurance to each type of platform, both as a dollar amount and as a percent of annual costs and expenses. The analysis includes four categories of costs. Age check costs are incurred to assure the age of a platform's existing user base. Annual age check costs are incurred to assure the age of the users that enter a platform each year. Annual compliance costs, presented estimated using the inputs in Table 11, are the costs necessary to sustain an age assurance apparatus, legally and technically, over a year. Fixed compliance costs, estimated using the inputs in Table 10, are the one-time costs necessary to construct that apparatus in compliance with the Act.[164] The tables below present the costs of age assurance by platform type. Aggregate estimates of fixed costs (one-time age check plus fixed compliance costs) and annual costs (annual age check plus annual compliance costs) are in the tables below.

[164] Age check costs are the sum of three items. Two are simple: (1) facial age estimation cost: cost per check (varies by platform) * number of users (2) document verification cost: percent of users who access waterfall stage 2 (0.18) * number of users * cost per check (varies by platform). The third, appeal cost, is more complex. (3) It is calculated by multiplying the number of users who fall to waterfall step 3 due to unsuccessful assurance ([1-0.82] * [1-0.95]) and by number of users and appeal cost. This provides one portion of the appeal cost. Next, the portion of all users who receive a false negative result from facial age estimation (0.01) is multiplied by the number of users successfully handled by facial age estimation (0.82), the number of users, and the cost. This is the second portion of the appeal cost. These two portions are added together, and multiplied by the percent of users who will not abandon the appeal process (estimated conservatively as the portion of users who do not abandon the document verification process, at 0.75). The sum of (1), (2), and (3) comprise a total estimate of age check costs. As above, these estimates on abandonment, accuracy, and cost come directly from information provided to OAG by age assurance providers. Annual age check costs use the same equation as age check costs but using annual user growth in place of annual users.

Annual compliance costs are calculated by multiplying the hour estimates for each platform by the wage estimates for each platform. Fixed compliance costs are calculated using the same equation but using fixed rather than annual costs.

One final caveat: "number of users" in this footnote does not refer to a platform's MAU in the U.S. (as, of course, only NY users need undergo age assurance). Instead, it refers to Annual Average Users (AAU) in New York. This parameter is estimated by dividing by the same ratio of NY users to U.S. users given above, and also multiplying by 3 to move MAU to AAU. This is likely a conservative overestimate of the scalar between MAU and AAU and thus likely a conservative estimate of the number of users who must undergo age assurance. *See* We Are Social, *Digital 2024: 5 Billion Social Media Users*, Jan. 31, 2024, https://wearesocial.com/us/blog/2024/01/digital-2024-5-billion-social-media-users (retention/turnover ratios).

Table 13: Platform 1 Age Assurance Costs

	Cost	Portion of Total Costs & Expenses
Age Check Costs	$2,419,311	0.04%
Annual Age Check Costs	$109,969	0.00%
Annual Compliance Costs	$262,400	0.00%
Fixed Compliance Costs	$144,800	0.00%
Algorithm Adjustment Costs	$93,600	0.00%
Fixed Costs	$2,657,711	0.04%
Annual Costs	$372,369	0.01%

"Cost" gives the cost in USD associated with the cost category in each row. "Portion of Total Costs & Expenses" expresses this cost in terms of the platform's simulated costs & expenses. These percentages, like all above and below, are expressed as decimals. (So, 0.01 is 1%.) See the paragraph above for descriptions of the cost categories in each row.

Table 14: Platform 2 Age Assurance Costs

Total Costs Model, Platform 2	Cost	Portion of Total Costs & Expenses
Age Check Costs	$779,821	0.17%
Annual Age Check Costs	$45,056	0.01%
Annual Compliance Costs	$95,000	0.02%
Fixed Compliance Costs	$58,600	0.01%
Algorithm Adjustment Costs	$36,000	0.01%
Fixed Costs	$874,421	0.19%
Annual Costs	$140,056	0.03%

"Cost" gives the cost in USD associated with the cost category in each row. "Portion of Total Costs & Expenses" expresses this cost in terms of the platform's simulated costs & expenses. See the paragraph above for descriptions of the cost categories in each row.

Table 15: Platform 3 Age Assurance Costs

Total Costs Model, Platform 3	Cost	Portion of Total Costs & Expenses
Age Check Costs	$157,704	0.46%
Annual Age Check Costs	$46,260	0.13%
Annual Compliance Costs	$46,900	0.14%
Fixed Compliance Costs	$30,600	0.09%
Algorithm Adjustment Costs	$18,900	0.05%
Fixed Costs	$207,204	0.60%
Annual Costs	$93,160	0.27%

"Cost" gives the one-time cost in USD associated with the cost category in each row. "Portion of Total Costs & Expenses" expresses this cost in terms of the platform's simulated costs & expenses. See the paragraph above for descriptions of the cost categories in each row.

Table 16: Platform 4 Age Assurance Costs

Total Costs Model, Platform 4	**Cost**	**Portion of Total Costs & Expenses**
Age Check Costs	$26,516	1.08%
Annual Age Check Costs	$13,258	0.54%
Annual Compliance Costs	$20,060	0.82%
Fixed Compliance Costs	$15,420	0.63%
Algorithm Adjustment Costs	$8,100	0.33%
Fixed Costs	$50,036	2.04%
Annual Costs	$33,318	1.36%

"Cost" gives the one-time cost in USD associated with the cost category in each row. "Portion of Total Costs & Expenses" expresses this cost in terms of the platform's simulated costs & expenses. See the paragraph above for descriptions of the cost categories in each row.

Table 17: Platform 5 Age Assurance Costs

Total Costs Model, Platform 5	Cost	Portion of Total Costs & Expenses
Age Check Costs	$8,264	1.20%
Annual Age Check Costs	$4,132	0.60%
Annual Compliance Costs	$12,000	1.74%
Fixed Compliance Costs	$10,600	1.54%
Algorithm Adjustment Costs	$6,000	0.87%
Fixed Costs	$24,864	3.61%
Annual Costs	$16,132	2.34%

"Cost" gives the one-time cost in USD associated with the cost category in each row. "Portion of Total Costs & Expenses" expresses this cost in terms of the platform's simulated costs & expenses. See the paragraph above for descriptions of the cost categories in each row.

Two important conclusions can be drawn from these estimates. First, compliance costs for large platforms are negligible as compared to their revenue and total costs. Second, as highlighted in the green cells in Tables 16 and 17, the fixed costs of age assurance become more expensive for platforms with fewer than 20,000,000 global MAU.

C. Aggregate Impact on Small Platforms

Parts IV.A and B together constitute a reasonable analysis of the costs of the Act to covered operators, including both the effect of the proscription against serving algorithmic feeds to minors and the costs of complying with the age assurance requirements, based on available data. This Part IV.C makes explicit the aggregate costs for small platforms. The lost advertising revenue model from Part IV.A is reiterated for small platforms specifically, with the conservative assumption that those platforms would be targeting advertising to minors prior to

the Act in order to maximize revenue. The results are added to those from Part IV.B to estimate the Act's total costs for small platforms.

1. Lost advertising revenue for small and very small platforms

Small platforms are platform types 4 and 5 described above with 1,000,000 and 300,000 U.S. MAU (2 million and 500,000 global MAU). In this section, platform type 4 is referred to as "small platforms" and type 5 as "very small platforms." The same model described in Part IV.A is applied to small platforms with a few adaptations. First, the estimate presented in Table 6 in Part IV.B for platform 4 revenue is used in place of the Big Six revenue figures. Scant information is available on the form and geographic location of small platform revenue. Thus, the estimate includes both the portion of revenue that is ad revenue and the percent of ad revenue derived from the U.S. as the average of those values for the Big Six.

Next, the small platforms are placed into three illustrative categories: (1) small minor population with a weak algorithm; (2) moderate minor population with an algorithm of normal strength; and (3) large minor population with a potent algorithm. Fewer minors are paired with weaker algorithms (and vice versa) not because these two dimensions are always correlated but to simulate an extreme higher and lower bound to these lost ad revenue estimates. To turn these generalizations about platform character into specific parameters for engagement decreases and the portion of revenue attributable to minors, estimates for the Big Six platforms in Part IV.A are used as the universe of possible values. For (1), the engagement decrease is assumed to be 0.13, and the portion of revenue attributable to minors is 0.02.[165] For (2), the engagement decrease is assumed to be 0.2 and the portion of revenue attributable to minors is 0.27.[166] For (3), the engagement bounds are set at 0.28.[167] The portion of revenue attributable to minors is assumed to be 0.42.[168]

For the smallest platforms, the same model is followed but with the estimate of platform 5 revenue taking the place of that of platform 4 revenue. For small and very small platforms, all other parameters, structural assumptions, and calculations mirror those performed in Part IV.A and B for platforms that currently target advertising to minors. The total advertising revenue lost from the SAFE for Kids Act's provisions, incorporating both a decrease in engagement and a

[165] The engagement decrease is that of Instagram, and the portion of revenue is that of Facebook, as stated in Table 2.

[166] Both values are from YouTube, as stated in Table 2.

[167] These are the values estimated for TikTok in Table 2.

[168] This is the actual value for Snapchat, as stated in Table 2.

decrease in spend on targeted advertising for both the small and smallest platforms, are presented in Tables 18 and 19.

Table 18: Small Platform Lost Ad Rev.

	Lost Ad Rev.	% of Rev.	% of Costs
Small Platform 1	67	0.000	0.000
Small Platform 2	1021	0.003	0.000
Small Platform 3	1800	0.005	0.001

"Lost Ad Rev" shows the revenue in USD lost by each platform type. "% of Rev" expresses that amount in terms of the platform's revenue, and "% of Costs" does the same for costs. These percentages are expressed as decimals. (So, 0.01 is 1%.)

Table 19: Smallest Platform Lost Ad Rev.

	Lost Ad Rev.	% of Rev.	% of Costs
Smallest Platform 1	17	0.000	0.000
Smallest Platform 2	255	0.003	0.000
Smallest Platform 3	450	0.005	0.001

"Lost Ad Rev" shows the revenue in USD lost by each platform type. "% of Rev" expresses that amount in terms of the platform's revenue, and "% of Costs" does the same for costs. These percentages are expressed as decimals. (So, 0.01 is 1%.)

Overall, even in the most extreme scenario (platform type 3), the advertising revenue losses due to the Act's provisions are negligible for small and very small platforms.

2. Total lost revenue & costs for small and very small platforms

Next, the lost advertising revenue estimates from Part IV.C.1 are added to the size-based age assurance cost estimates from Part IV.B, presented in Tables 16 and 17, to determine the cumulative impact of the Act on small and very small platforms. The cost of age assurance will not vary based on the same variables affecting the changes in revenue in Part IV.C.1. To avoid reporting an overwhelming number of estimates and because the effects on revenue from lost advertising revenue are negligible across platform types, the second scenario shown in the tables above is used to determine the totals. Total costs for both small and very small platforms are displayed in the table below.

Table 20: Total Lost Revenue & Costs for Small and Very Small Platforms

	Small Platform	Portion of Costs	Smallest Platform	Portion of Costs
Lost Ad Rev.	$1,021	0.0%	$255	0.0%
Annual Costs	$33,318	1.4%	$16,132	2.3%
Fixed Costs	$50,036	2.0%	$24,864	3.6%
Total Annual Loss	**$34,339**	**1.4%**	**$16,387**	**2.4%**
Total Fixed Loss	**$50,036**	**2.0%**	**$24,864**	**3.6%**

Rows: "Lost Ad Rev" shows the total ad revenue lost from the Act. "Annual Age Assurance Costs" come from the "Annual Costs" estimate in Tables 12-15 above. "Fixed Age Assurance Costs" come from the "Fixed Costs" estimate in Tables 12-15 above. "Total Annual Loss" displays the total annual cost of the Act, including both ad revenue loss and age assurance costs. Columns: "Small Platform" displays costs in USD for small platforms. "Portion of Costs" shows this number as a percent of total annual costs & expenses. The next two columns do the same for very small platforms.

3. Threshold for commercial reasonability

These calculations bear on the issue of a threshold based on a metric, be it users, revenue, or costs, below which highly accurate age assurance techniques would be potentially commercially infeasible for platforms. The industrial context that covered operators inhabit is not conducive to a threshold based on either revenue or costs. First, platforms with a low to moderate user count often intake little revenue. So, a revenue threshold might exempt platforms with a high number of users that expose a substantial number of minors to addictive feeds. Second, regulations that categorize companies on the basis of costs rather than revenue are somewhat rare. In part, that is because such an exemption would introduce perverse incentives for firms to keep costs just below a certain threshold. A more feasible option is to link a threshold exemption to the number of users on a platform. Such a threshold also ensures that exempt entities are not subjecting large numbers of minors to addictive feeds without the protections of the Act.

The age assurance compliance cost estimates in Part IV.B. shed light on the appropriate magnitude of a user threshold. These estimates show that stringent age assurance requirements pose a negligible financial burden on large platforms, both in terms of fixed and recurring costs. Between the platform types 3 and 4 (20,000,000 and 2,000,000 global MAU), there is a discontinuous leap in the relative size of the fixed and recurring costs necessary to comply with the Act. While compliance is commercially reasonable for platforms similar to type 3, it may not be so for platforms similar to type 4.

Ability to bear the costs associated with the Act is one factor relevant to setting the threshold. Another factor is the number of minors exposed to addictive feeds on platforms below the threshold. A platform with 1,000,000 U.S. MAU (equivalent in the analysis herein to 2,000,000 global MAU) would likely serve between 1,000 to 20,000 New York minors each

month.[169] By contrast, a platform with 10,000,000 U.S. MAU (equivalent to 20,000,000 global MAU) would likely serve 10,000 to 200,000 New York minors each month.[170]

The OAG conducted a sensitivity analysis to better understand the relative commercial feasibility of age assurance for platforms with between 5 and 15 million global MAU. This also requires estimating revenue for the different sized firms: 15 million, 10 million, and 5 million global MAU.[171]

Table 21: Platform Financials for Platforms with Global MAUs of 5, 10, and 15 million

Other Info	**15 M**	**10 M**	**5 M**
SWE wage	$70	$60	$54
Legal wage	$350	$300	$250
Business wage	$60	$55	$50
Customer service wage	$25	$25	$25
Number of NY AAU	858,125	686,500	429,062
Number of US MAU	5,000,000	4,000,000	2,500,000
Number of Global MAU	15,000,000	10,000,000	5,000,000
Total annual costs & expenses	$25,937,039	$9,440,390	$2,988,889
Revenue	$17,867,647	$6,844,771	$888,889
Annual US user growth	2,933,333	2,346,667	1,466,667
NY user growth	167,811	134,249	57,208

[169] 1,000,000 (MAU) * 0.06 (ratio of NY to U.S. users) * either 0.02 or 0.4 (the portion of ad revenue attributable to minors, a proxy for the number of minors on the social media platform).

[170] The same calculation as above for 10,000,000 MAU.

[171] The estimates for the platform with 15 million global MAU ("15M platform") are produced in a very similar fashion to the 20M platform. The wage estimates are all identical, as is the scalar between US and global MAU, as is that between global MAU and revenue, and that between revenue and costs. The same is true for the 5M platform with respect to the 2M platform in the financials estimates in Part IV.B for a very small platform. The wage estimates are all identical, as is the scalar between US and global MAU, the method for deriving revenue from users, and costs from revenue. The user growth rate is equal for all three sensitivity test platforms.

Because the 10M platform is on the border between the small, nearly-non-monetizable platforms and the mid-size, somewhat-monetizable platforms, rather than using the scalar from one or the other, the analysis averages the two. The multiplier between US and global MAU is the average of that for the 5M and 15M platforms. The RPU number is the average of that for the 10M-70M range and that for the 0-70M range. The cost estimate also averages the two distinct methods for the 5M and 15M platforms.

Based on these financials, OAG estimates the total costs and costs as a percentage of total costs and expenses to better understand a potential threshold for commercial feasibility.

Table 22: Costs and % of Total Costs for Platforms with Global MAUs of 5, 10, and 15 mil

15M Global MAU	**Cost**	**% of Total Costs & Expenses**
Age Check Costs	$177,417	0.68%
Annual Age Check Costs	$34,695	0.13%
Annual Compliance Costs	$46,900	0.18%
Fixed Compliance Costs	$30,600	0.12%
Algorithm Adjustment Costs	$18,900	0.07%
Fixed Costs	$226,917	0.87%
Annual Costs	$81,595	0.31%
10M Global MAU	**Cost**	**% of Total Costs & Expenses**
Age Check Costs	$141,934	1.50%
Annual Age Check Costs	$27,756	0.29%
Annual Compliance Costs	$40,200	0.43%
Fixed Compliance Costs	$26,550	0.28%
Algorithm Adjustment Costs	$16,200	0.17%
Fixed Costs	$184,684	1.96%
Annual Costs	$67,956	0.72%
5M Global MAU	**Cost**	**% of Total Costs & Expenses**
Age Check Costs	$88,709	2.97%
Annual Age Check Costs	$11,828	0.40%
Annual Compliance Costs	$34,180	1.14%
Fixed Compliance Costs	$23,940	0.80%
Algorithm Adjustment Costs	$14,580	0.49%
Fixed Costs	$127,229	4.26%
Annual Costs	$46,008	1.54%

Based on these costs and as discussed in Part III.B, OAG proposes a threshold of over 5 million global MAUs as an appropriate threshold over which it is commercially reasonable for platforms to comply with the requirements of the Act. While relative costs at this threshold are not as low as they are for much larger platforms, they decline as a platform reaches 10 million global MAU. Moreover, given the exemption for platforms with fewer than 20,000 minor users in New York, this threshold will appropriately target online platforms whose reach is 3,000 to 60,000 New York minors based on the OAG's estimate of the number of minor users associated with a platform that has 5 million global MAU. Moreover, online platforms entering the market

may choose to design platforms that are more amenable to being adjusted to operate without an unlawful engagement algorithm to the extent they plan to grow a user-base in New York.

D. Costs of a parental consent system

The Act allows covered operators to provide a method of parental consent and directs OAG to promulgate rules implementing parental consent.[172] Covered operators, however, are not required to provide for parental consent under the Act or the proposed rule. It is optional and therefore any costs associated with implementing the parental consent provisions are also optional under the statute and the proposed rule. As a consequence, section 202-A(c) of the State Administrative Procedure Act does not require OAG to detail the projected costs to regulated parties of the parental consent provisions.[173] In considering the available policy options, however, OAG considered the costs and economic effects of those options in crafting the proposed rule, and in the interest of completeness and transparency, this section provides cost information related to the parental consent provisions of the proposed rule.

When the COPPA Rule first became effective in 2000 in the U.S., the underlying technologies for available parental consent methods were not nearly as advanced as they are today, and they were less cost-effective. With existing methods already present and proven, market forces will likely continue to push any new forms of parental consent to be cheaper. Notably, a 2025 technology trial report commissioned by the Australian government found that multiple parental consent management vendors have technology readiness levels ranging from viable pilot technology to a viable, commercially available product, demonstrating that such technologies are accessible and more will shortly be accessible to operators at commercial pricing.[174]

1. Cost information on implementing a method of parental consent

For purposes of analyzing the costs of incorporating methods of parental consent, as an upper bound, OAG assumes all covered operators will provide a method for parental consent

---

[172] G.B.L. § 1501(4).

[173] State Admin. Pro. Law § 202-A(c).

[174] Age Check Certification Scheme, *Age Assurance Technology Trial Final Report: Part H – Parental Consent* 63 (August 2025), https://www.infrastructure.gov.au/sites/default/files/documents/aatt_part_h_digital.pdf. The trial assessed 12 parental consent vendors offering a variety of methods. As the trial and the report were both commissioned in preparation for Australia's implementation of its own specific age-assurance measures for online platforms, the participating providers were assessed based on their readiness against Australian legal requirements, with any additional compliance with laws such as COPPA noted but not the focus of the assessment. *Id.* at 18-27. Accordingly, the report offers helpful insight into the readiness state and availability of non-COPPA parental-consent methods.

and will therefore incur related costs. The structure of parental consent in the proposed rule and COPPA is similar.[175] Both include requirements for parental consent methods, such as verifying a parent's status as a parent, providing the parent with a mandatory notice, and presenting the parent with an opportunity to grant or refuse valid consent.[176] Moreover, at least some covered operators under the Act must also comply with COPPA and can be presumed to have implemented COPPA's verifiable parental consent mechanisms. In its COPPA rulemakings, the FTC has analyzed the costs associated with verifiable parental consent methods, including the cost of preparing COPPA's mandatory parental notice.[177] Thus, OAG looks to the FTC's cost estimates for implementing COPPA-compliant parental consent methods and the mandatory COPPA notice to estimate certain costs incurred by covered operators under the Act. [178]

The FTC finalized its most recent amendment to the COPPA Rule in April 2025. The amended final rule estimates a new market entrant would use 60 total hours to prepare and implement COPPA-compliant notices and parental consent mechanisms.[179] The FTC concludes this time would be allocated at a 5:1 ratio of legal drafting and review (50 hours) to technical implementation (10 hours).[180] The FTC estimates rates for legal and technical work at $655/hour for legal counsel and $60.43/hour for technical personnel.[181]

This analysis presents costs for two categories of covered operators—covered operators who also must comply with COPPA and covered operators who are not required to comply with COPPA. The two will likely incur different costs. For covered operators who must comply with

---

[175] *Compare* sections 700.2(d) and 700.3(d) with COPPA Rule, 90 Fed. Reg. 16918, 16980-81 (Apr. 22, 2025).

[176] *Id.*

[177] COPPA Rule, 90 Fed. Reg. 16918, 16971-77 (Apr. 22, 2025); COPPA Rule, 78 Fed. Reg. 3972, 4000-4008 (Jan. 17, 2013).

[178] While it is possible for covered operators to use methods that do not comply with COPPA, this analysis assumes that covered operators would only do so if the costs of such methods were lower. The OAG is not aware of such systems or their lower costs. However, this analysis, which uses COPPA as a proxy may, thus, inflate the actual cost and provides an upper bound.

[179] COPPA Rule, 90 Fed. Reg. 16918, 16973 (Apr. 22, 2025).

[180] COPPA Rule, 90 Fed. Reg. 16918, 16974 (Apr. 22, 2025).

[181] COPPA Rule, 90 Fed. Reg. 16918, 16974 (Apr. 22, 2025). The OAG estimates legal and technical wages and expenses for different size platforms in Table 7 in Part IV.B.1 as part of its analysis of the age assurance requirement. As noted, the wages presented in Table 7 of Part IV are illustrative examples and not strict or weighted averages or estimates. Thus, this analysis uses the FTC's estimates to estimate total costs associated with parental consent. Notably, the FTC's wage estimates are consistent with the ranges estimated in Table 7.

both COPPA and the Act, the proposed rule allows the use of COPPA-compliant consent methods and a combined COPPA-SAFE for Kids Act notice process as part of a single transaction.[182] Thus, covered operators who comply with COPPA would not incur a separate cost for implementing parental consent methods or creating a notice flow from scratch. Instead, their costs would be limited to the cost of the additional requirements of the proposed rule, which include creating the notice required by the proposed rule and translation requirements for the notice.[183] On the other hand, covered operators who are not required to comply with COPPA will incur costs similar to market entrants newly setting up a COPPA compliance program together with the cost of some additional requirements of the proposed rule, although as explained further, the notice obligation under COPPA is more complex than the notice required by the proposed rule.[184]

This analysis first turns to covered operators who are already complying with COPPA. Based on prior estimates of COPPA compliance costs, the similarities between the two schemes, and OAG's expertise, OAG preliminarily estimates that preparing the initial English-language notice in the proposed rule would take no more than two hours of legal work and one hour of technical implementation. The Act and proposed rule require translation for notices and instructions related to providing parental consent, which COPPA does not mandate.[185] The OAG estimates that covered operators would use an additional 5 hours for each language version of the notice and instructions in total, allocated at a 2:1 ratio between translation services and technical personnel, for a total of 55 hours across 11 language versions (counting the initial English-language version among the 12 statutorily-required languages).[186] Using U.S. Bureau of Labor Statistics data, OAG estimates a rate of $41.73/hour for translation services.[187] The rate

---

[182] Part III.B.3.b.iii discusses how covered operators may comply with both COPPA and the Act.

[183] *See* Part III.B.3.b.iii for further discussion of the additional requirements.

[184] *Compare* COPPA Rule, 90 Fed. Reg. 16918, 16973, 16978-980 (Apr. 22, 2025) *with* section 700.2(d)(5).

[185] G.B.L. § 1506; sections 700.2(e)(6) and 700.3(e)(6) of the proposed rule.

[186] The proposed rule clearly outlines the minimum requirements for notice text. The OAG thus estimates that a compliant notice can be 250 words or less, using common, non-technical language that does not require specialist translation services. The technical work required to set up each language version of the notice will be identical, save for loading in different text and conducting separate testing for each version to ensure proper display (although the tests themselves will be identical). Accordingly, a two to one ratio appropriately reflects that the technical work will take less time than the translation work.

[187] Bureau of Labor Statistics, Occupational Employment and Wage Statistics: Occupation – Interpreters and Translators (SOC code 27-3091), New York (May 2024) via the Occupational Employment and Wage Statistics Query System tool available at https://data.bls.gov/oes/#/home.

for technical personnel remains the same as that reported by the FTC, namely $60.43 per hour.[188]

In total, OAG estimates that implementing a parental consent mechanism under the Act and proposed rule would cost approximately $4,008 per online platform that complies with COPPA. Under the proposed rule, a covered operator who implements a COPPA-compliant verifiable parental consent method must also take reasonable steps, in light of available technology, to account for the likelihood that the method will be circumvented, misused, or subject to fraud.[189] The FTC routinely considers similar criteria when reviewing parental consent methods and has cautioned operators to take account of them or risk enforcement actions.[190] Thus, this requirement is not likely to result in a significant additional burden or implementation costs for covered operators required to comply with COPPA.

For covered operators who are not required to comply with COPPA, OAG assumes that existing covered operators have no other parental consent mechanisms set up, again as an upper bound.[191] The OAG preliminarily estimates that the required hours of legal services to prepare the notice required by the proposed rule will be five hours. The OAG estimates that legal counsel reviewing the Act's requirements and drafting an appropriate notice as a standalone project may need more time than the two hours estimated when working on a combined COPPA-SAFE for Kids Act project, as they would not be able to consolidate tasks or rely on prior implementation plans and existing expertise. However, as COPPA's notice requirements are significantly more extensive than those in the proposed rule, it is reasonable to estimate a much lower number than the 50 hours needed for the COPPA notice alone.[192]

A standalone SAFE for Kids Act notice will likely require the same technical resources as implementing a combined COPPA-SAFE for Kids Act notice, so the same estimate can be used as

---

[188] COPPA Rule, 90 Fed. Reg. 16918, 16974 (Apr. 22, 2025).

[189] Sections 700.2(d)(6)(v) and 700.3(d)(6)(v).

[190] *See, e.g.*, COPPA Rule, 90 Fed. Reg. 16918, 16951-53 (Apr. 22, 2025) (to be codified at 16 C.F.R. § 312) (discussing potential for types of fraud committed by child users using a verifiable parental consent method and misuse of data collected from the parent).

[191] A covered operator who is not governed by COPPA may elect to implement an FTC-approved COPPA-compliant method of verifiable parental consent, provided that the covered operator complies with all provisions of the proposed rule as noted in Part III.B.3.b.iii. As this does not change notice requirement required by the proposed rule, the cost estimates in this paragraph are the same regardless of the method of parental consent the covered operator chooses.

[192] *Compare* COPPA Rule, 90 Fed. Reg. 16918, 16973, 16978-980 (Apr. 22, 2025) *with* section 700.2(d)(5).

an upper bound on technical costs.[193] Similarly, the translation costs for a standalone notice and accompanying instructions will not be appreciably different since only the SAFE for Kids Act-mandated portion is translated in either case. Accordingly, OAG estimates 5total hours for each language version, allocated at a ratio of 2:1 between technical and translation work, or 55 hours in total. All hourly rates (legal, technical, translation) would remain the same across these preliminary estimates. The OAG thus estimates that it would cost approximately $5,973 per online platform for the covered operator to draft and implement a notice complying with the proposed rule.

Lastly, this analysis assumes covered operators will spend an additional 25% of the initial costs for continued compliance and maintenance[194] including costs related to the proposed rule's requirements to make reasonable efforts to consider parents' and covered minors, privacy and safety and to be reasonably calculated in light of available technology to account for the likelihood of circumvention, fraud or misuse of the method[195] This results in an estimated cost

---

[193] The technical support requirements will be substantially the same as for a combined notice as only the language and the timing of a standalone notice would be different from a combined notice. Additionally, a covered operator is likely to have the necessary technical support personnel and expertise, since the technical requirements are very similar to those required to provide other types of legal notices to users, such as Terms of Service changes.

[194] In its analysis of costs associated a UK law requiring age assurance, an estimate from UK's regulator for communication services, applies a default rate of 25 percent of initial costs for ongoing maintenance costs, including costs related to privacy and fraud detection. Ofcom, Protecting Children from Harms Online Annexes 10-15 26 (2024), https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/284469-consultation-protecting-children-from-harms-online/associated-documents/a10-15-other-annexes.pdf?v=33607. A 25 percent cost is added to the cost of implementing parental consent for covered operators who are not required to comply with COPPA but is not applied for covered operators already complying with COPPA given COPPA's existing requirements.

[195] The FTC also considers several of these criteria when evaluating a proposed method of verifiable parental consent. *See, e.g.*, COPPA Rule, 90 Fed. Reg. 16918, 16951-53 (Apr. 22, 2025). However, FTC approvals for these methods are granted in context of COPPA, which only applies to children under the age of 13. COPPA, 15 U.S.C. § 6501(1) (defining "child" as an individual under 13). Several of the FTC's approvals also predate the start of the rulemaking for the latest revisions to the COPPA Rule in 2019, and were thus granted in light of the available technology at the time. FTC, *Verifiable Parental Consent and the Children's Online Privacy Protection Rule*, https://www.ftc.gov/business-guidance/privacy-security/verifiable-parental-consent-childrens-online-privacy-rule (Imperium approval granted Dec. 23, 2013 and Riyo approval granted Nov. 19, 2015). The proposed rule recognizes that both the available technology and criteria such as user safety may differ when considering children aged 13-17 and accordingly accounts for this additional cost based on an estimate of costs related to an age assurance requirement in the U.K that applies to all individuals under 18. Ofcom, Protecting Children from Harms Online Annexes 10-15 26 (2024), https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/284469-consultation-protecting-children-from-harms-online/associated-documents/a10-15-other-annexes.pdf?v=33607. For covered minors aged 13-17, a covered operator can certainly consider methods of verifiable parental consent approved by the FTC under the COPPA Rule (and OAG expects that some or all methods may also satisfy the proposed rule when paired with additional technology), but must analyze the methods for compliance with the proposed rule's criteria.

per platform of $7,466 and is an upper bound as the covered operator must implement an appropriate parental consent method in conjunction with an appropriate age assurance method and costs will likely be consolidated. Any remaining additional costs for implementing the method of verifiable parental consent should be only incremental to the covered [196] since the same technical staff and resources would be needed as for age [197]

2. Age assurance cost information

Next, the covered operator would incur the cost of conducting age assurance on the purported parent consistent with the proposed rule.[198] This cost is calculated for the same hypothetical addictive online platforms of five different sizes as the cost of age assurance in Part IV.B.2. The cost for each parent is equal to the cost of putting one more user through age assurance as estimated in Part IV.B.2. All costs associated with implementing and maintaining age assurance methods are already accounted for in that Part as the costs of implementing age assurance for users. They are not counted again in this analysis.

Not all covered minors will seek parental consent and not all parents being asked for consent will choose to provide that consent. Therefore, the number of parents undergoing age assurance for purposes of providing parental consent will be a fraction of the number of

[196] Project scoping and user testing are discussed in Part IV.B.2 as part of OAG's age assurance cost analysis. Implementation of a parental consent method would similarly require project scoping and user testing, and a covered operator who decides to offer a parental consent method would need to carry these tasks out at the same time as it does for age assurance and ensure the method is integrated with age assurance. It is therefore reasonable to assume that the covered operator will consolidate staffing and other resources for both projects as much as possible.

[197] A covered operator who is not governed by COPPA may elect to implement a method of verifiable parental consent that has not been reviewed under the approval mechanism set out in section 312.12(a) of the COPPA Rule. This analysis assumes a covered operator maintains their existing COPPA consent method because it is likely to be cost-effective.

[198] The OAG also notes that the proposed rule incorporates a reasonableness standard for determining who is a parent, as does the COPPA Rule. 16 C.F.R. §§ 312.2 (definition of "obtaining verifiable consent"), 312.5. Implementation costs may also be attributable to the proposed rule's requirements to include at least one option that does not require the parent to furnish government-provided identification and to provide at least one option that does not require the parent to create an account with the covered operator or to purchase additional goods or services from the covered operator. However, these costs are dependent on what method(s) of parental consent the covered operator decides to implement and may not necessarily be incurred solely due to the Act, since the COPPA Rule does not limit the covered operator to a single verifiable parental consent method. *See* 16 C.F.R. § 312.5.

covered minors.[199] To calculate the relative number of age checks for parents, OAG relies on certain assumptions.

First, OAG assumes operators complying with COPPA will rely on COPPA-compliant methods of verifiable parental consent consistent with sections 700.2(e)(6) and 700.3(e)(6) of the proposed rule. COPPA does not require an explicit age assurance step for parents.[200] Accordingly, the cost estimate does not include any parental consent age checks for covered minors under 13.

Next, OAG calculates the percent of all covered users that are covered users aged 13 to 17, *i.e.*, the universe of minor users that might request parental consent, which is equal to 5.843%.[201] The OAG assumes that approximately one-third of these covered users aged 13 to 17 will seek parental consent. The OAG further assumes that approximately 25% of parents receiving a request for parental consent will then initiate a parental consent mechanism and undergo age assurance. As discussed further, the OAG believes the latter two assumptions are reasonable estimates – based on available data about user behavior in analogous circumstances – that likely overestimate the number of parents that will undergo age assurance.

For several reasons, not all covered minors will request parental consent for addictive feeds or nighttime notifications. For example, not all covered minors may wish to access an addictive feed or nighttime notifications. Some parents may not be aware of their children's use of online platforms with addictive feeds and the minor may not want to alert the parent of their use. Minors may also know that their parents will not consent and, thus, not bother with the request. Thus, the number of covered minors who will validly consent to the operator sending a request for parental consent on their behalf consistent with sections 700.2(e) and 700.3(e) will

---

[199] The OAG also assumes that for each covered minor, no more than one individual will be initially identified as a parent and will be sent a request for parental consent, since as discussed in Part III.B, the proposed rule only requires that one parent grant consent for a covered minor to access an addictive feed or nighttime notifications.

[200] While an operator may choose to offer COPPA-compliant methods alongside other, non-COPPA compliant methods, OAG assumes that the operator would only do so if the total costs were less than adjusting a COPPA-compliant method to also comply with the Act, which is discussed in more detail in Part III.B.4.b.iii.

[201] The OAG assumes the rate of social media use among adults is the same as the rate of social media use by 13- to 17-year-olds. *See* U.S. Surgeon Gen. Advisory, *Our Epidemic of Loneliness and Isolation* 20 (2023). Therefore, the percentage of all covered users that are covered minors aged 13 to 17 is the same as the percent of the population of all New Yorkers (19,867,248) that are New Yorkers aged 13 to 17 (1,160,798), which is 1,160,798/19,867,248, resulting in 5.843%. U.S. Census Bureau, *Annual Estimates of the Resident Population by Single Year of Age and Sex: April 1, 2020 to July 1, 2024 (SC-EST2024-SYASEX)*, https://www.census.gov/data/datasets/time-series/demo/popest/2020s-state-detail.html.

be lower than the total number of covered minors using the addictive online platform.

The OAG believes that its one-third assumption is an upper bound estimate. This estimate is derived from surveys directly asking minors such questions as whether they have used a platform safety tool or feature[202], whether they have taken steps to actively manage the content they see on a platform[203], whether they have used a platform tool or feature to track their usage time[204], and whether they have taken steps to reduce or stop use of a platform themselves[205]. These studies indicate that between 60% and 80% of minors take some active steps to manage their use of an online platform. The OAG also reviewed a study indicating that 26% to 40% of minors have talked to a parent or caregiver about a platform safety issue, which may indicate comfort with some level of parental involvement in the minor's online activities, and thus, reflect on the likelihood a minor might at least discuss consent with a parent.[206]

Similarly, OAG's estimate that 25% of parents who receive a request for parental consent will then initiate a parental consent mechanism and undergo age assurance is also an overestimate. If a parent chooses not to consent in the first instance, then they will not undergo age assurance and the operator will not incur the related costs of age assurance. Similarly, a parent may begin the consent process but later decide against it before undergoing age assurance. There is strong evidence that parents have concerns about social media use and its effects on the mental health of minors as outlined in Part II. For example, over 80% of U.S.

---

[202] Thorn, *LGBTQ+ Youth Perspectives: How LGBTQ+ Youth Are Navigating Exploration and Risks of Sexual Exploitation Online* 41 (2023), https://info.thorn.org/hubfs/Research/Thorn_LGBTQ+YouthPerspectives_June2023_FNL.pdf (64-84% of minors aged 13-17 have done so).

[203] Common Sense Media, *A Double-Edged Sword: How Diverse Communities of Young People Think About the Multifaceted Relationship Between Social Media and Mental Health* 30-31. (2024), https://www.commonsensemedia.org/research/double-edged-sword-how-diverse-communities-of-young-people-think-about-social-media-and-mental-health (61% of individuals aged 14-22 have done so).

[204] Digital Wellness Lab, *The Digital Wellness Lab's Pulse Survey – Adolescent Media Use: Attitudes, Effects, and Online Experiences* 12 (2022), https://digitalwellnesslab.org/wp-content/uploads/Pulse-Survey_Adolescent-Attitudes-Effects-and-Experiences.pdf (57.% of minors aged 13-17 have done so).

[205] Common Sense Media, *A Double-Edged Sword: How Diverse Communities of Young People Think About the Multifaceted Relationship Between Social Media and Mental Health* 33. (2024), https://www.commonsensemedia.org/research/double-edged-sword-how-diverse-communities-of-young-people-think-about-social-media-and-mental-health (over 60% of minors have tried to reduce platform use or have deleted accounts).

[206] Thorn, *LGBTQ+ Youth Perspectives: How LGBTQ+ Youth Are Navigating Exploration and Risks of Sexual Exploitation Online* 45 (2023), https://info.thorn.org/hubfs/Research/Thorn_LGBTQ+YouthPerspectives_June2023_FNL.pdf.

adults favor parental consent and time restrictions for minors using social media sites.[207] Parents sharing this concern will be less likely to provide consent. The OAG also considered data related to opt-in mechanisms implemented under privacy laws in other jurisdictions, which routinely yield consent rates between 20% and 40%.[208] The OAG preliminarily concludes parental initiation rates are likely to be on the lower end of this rage.

The cost of age checks for parental consent is then calculated per hypothetical platform based on these assumptions and the total cost for all age checks and annual age checks reported in Tables 13 through 17 in Part IV.B.2. OAG estimates age checks for parents will result in costs ranging from a total of $12,315 for the largest covered hypothetical platform type (Platform 1) to $993 for the smallest covered hypothetical platform type covered by the proposed rule (Platform 3).[209] These costs are an extremely small fraction of such platforms' current estimated costs. The total costs and expenses of Platform 1, a very large platform are estimated to be almost $6.15 billion in Table 6 of Part IV.B.1—parental consent age checks would add a total of $12,315. For Platform 3, OAG estimates in Table 6 that total costs and expenses will total approximately $2.45 million and parental age checks would total $993.

---

[207] Pew Research Center, Social media policies for minors: What US adults and teens think | Pew Research Center. Many surveys have demonstrated that parents are interested in reducing or otherwise managing minor use of addictive online platforms. *See, e.g.,* CBS News, *89% of parents support laws restricting kids from social media, survey found*, (June 27, 2023), https://www.cbsnews.com/miami/news/89-of-parents-support-laws-restricting-kids-from-social-media-survey-found/. A Gallup poll reported that about half of all parents surveyed currently impose screen time restrictions, presumably restrictions the parents were required to initiate rather than consent to based on the timing of the poll. Jonathan Rothwell, *Teens Spend Average of 4.8 Hours on Social Media Per Day* (October 13, 2023),

[208] *See, e.g.*, Rita Heimes, *How opt-in consent really works* (Feb. 22, 2019), https://iapp.org/news/a/yes-how-opt-in-consent-really-works/ (observing cookie consent rate of 34% in response to GDPR); Empower, *How to benchmark your GDPR opt-in rates (aka re-permissioning)* (June 28, 2018), https://empower.agency/how-to-benchmark-your-gdpr-opt-in-rates-aka-re-permissioning/ (quoting post-GDPR opt-in rates for nonprofit and for-profit companies in the UK.

[209] To estimate these costs the ratio of New York minors ages 13 to 17 to the total New York population, 5.843%, is first multiplied by the fraction of those minors that will seek parental consent (1/3) and then multiplied by the fraction of parents that will go the age assurance process to consent (25%). This results in a total of 0.487%. In other words, 0.487% of the total population of covered users will have a parent that goes through age assurance to provide parental consent. The OAG assumes one parent will go through the age assurance process for each minor. In other words, operators will have to conduct an extra age check for parents of these users equal 0.487% of the total number of users. Because the cost per user is equally distributed, the same percentage can be applied to the total cost of all age checks. Thus, the costs of age checks and annual age checks are added together for Platform 1 ($2,419,311 + $109,969) and Platform 3 ($157,704 + $46,260), respectively. *See* Tables 13 and 15 in Part IV.B.2, respectively. Each sum is then multiplied by 0.487% resulting in a marginal cost for age assurance checks for parental consent of $12,315 for Platform 1 and $993 for Platform 3, respectively.

V. Alternatives

As discussed throughout this regulatory impact statement, OAG carefully considered alternatives for the provisions in the proposed rule and the different interests of the parties affected by those alternatives. The OAG proposes the rule based on its preliminary determination that the proposed rule best implements the Act consistent with its authority and the Legislature's intent while balancing those interests.

A. Scope of the proposed rule

OAG considered several ways to quantify the meaning of "significant part" to best effectuate the Act's intent, including the number of users of the addictive feed compared to the number of users of the online platform generally and the revenue attributable to the addictive feed as a portion of the online platform's total revenue. As discussed in Part III.A, each of these metrics present compelling reasons why they may not accurately reflect whether an addictive feed is a "significant part" of an online platform. Accordingly, OAG did not incorporate them into the proposed rule.

Similarly, the proposed rule defines exempt addictive online platforms based on the Act's requirement that age assurance measures be commercially reasonable and technically feasible. An exempt addictive online platform is determined in part by measuring its monthly active users. In defining monthly active user for this purpose, OAG researched a wide range of industry methods for calculating monthly active users and found little consistency across methods. Accordingly, rather than choosing any specific existing method of calculation, the proposed rule reflects a straightforward definition of monthly active user as discussed in Part III.A.

The OAG also considered but ultimately rejected proposing several other thresholds for this exemption, such as thresholds based on annual revenue and the amount of time users spend on the platform. As discussed in Parts III.A, B, and D, OAG preliminarily finds that these alternatives would not be as practical to implement and may exclude online platforms with large numbers of covered minors.

B. Age assurance

The proposed rule's provisions on age assurance intend to provide clear, practical guidance as to what types of age assurance satisfy the Act. The OAG considered providing a list of acceptable age assurance methods as an alternative to the proposed rule's approach of specifying technical minimum standards, but proposed the latter standard based on their practicality and flexibility. The proposed rule's standards also allow for covered operators and third-party providers to continue to innovate, as discussed further in Parts III.B and D.

The OAG also considered several models for evaluating age assurance methods, including a single accuracy minimum threshold across all ages, but preliminarily finds that a tiered accuracy minimum thresholds for several age groups best balances all considerations for the reasons discussed in Parts III.A, B, and D. Also reviewed as alternatives were various specific accuracy thresholds for each age-group. After examining the available information for a wide range of age assurance methods, OAG preliminary finds that the thresholds set forth in the proposed rule reflect the current state of the art while balancing the factors mandated by the Act.

Separately, OAG considered whether self-declaration and third-party vouching should be considered methods of age assurance capable of meeting the Act's objectives and preliminarily finds that they cannot. Although self-declaration is currently widely used, it has known accuracy issues. Third-party vouching similarly has not been proven to be sufficiently reliable. These issues are further discussed in Part III.D.

C. Parental consent

When proposing the provisions on parental consent, OAG considered whether covered operators should be able to require a parent to create an account with the covered operator or to pay even a nominal fee to use a method of parental consent. The OAG determined that neither condition was technically necessary and, if imposed, both could unfairly burden and discriminate against certain users, as discussed in Parts III.B.4 and C.3 addressing parental consent.

The OAG also examined the use of verifiable parental consent methods approved by the FTC under the COPPA Rule for online platforms governed by the Act, particularly for covered operators not subject to COPPA. As discussed in detail in Part III.B addressing parental consent, OAG proposes a careful approach to ensuring a covered operator may streamline efforts to comply with the Act and with COPPA whenever possible. But OAG declines to replicate COPPA in the proposed rule to ensure the rule is consistent with the Act's mandates and intent.

VI. Paperwork

The proposed rule contains no reporting requirements. The OAG is proposing that covered operators be obligated to maintain "all test results, reports, and certifications" generated in compliance with Section 700.5 for a minimum of 10 years, *see* section 700.5(d). Additionally, under the proposed rule, covered operators will be obligated to maintain data related to the conduct of age assurance and related information pursuant to section 700.7(b) for a minimum of 10 years. This data is necessary to ensure covered operators' compliance with the requirements of the proposed rule.

VII. Regulatory Flexibility Analysis for Small Business and Local Governments

The proposed rule requires a covered operator of an addictive online platform to implement an age assurance method to determine if a user is a covered minor, and if so, to deny that covered minor access to addictive feeds and nighttime notifications unless the covered operator has obtained verifiable parental consent. The Act also includes other provisions, including requirements related to data deletion and providing access to minors to covered online platforms without addictive feeds. The proposed rule includes provisions to facilitate implementation of these and other provisions of the Act.

The proposed rule will not affect local governments. Local governments will not have to undertake any reporting, recordkeeping, or other affirmative acts to comply with the proposed rule since it does not apply to a local government.

The proposed rule excludes operators that either serve fewer than 20,000 New York minors or have fewer than 5,000,000 global users based on the preliminary determination in Part IV that the cost of compliance with the requirement to conduct age assurance may be relatively burdensome for such operators. A minimal number of small businesses as defined by section 102(8) of the State Administrative Procedure Act may reside in New York and be covered under the proposed rule nevertheless. OAG has estimated the potential costs to small and very small platforms, including a sensitivity analysis of platforms with sizes in between, and does not believe the proposed rule will have a substantial adverse impact on small businesses.

The minimal number of small businesses that may be covered by the Act under the proposed rule will be required to comply with it. In the unlikely event a small business is a covered operator, it may require the professional services of an attorney, a technical engineer, and a person with business development skills as described in Part IV.C. Although unlikely, a covered operator that may be a small business may other incur costs consistent with the analysis in Part IV. A covered operator that may be a small business will not face economic and technical feasibility issues based on the analysis completed by OAG in Part IV as age assurance technology is readily available from third parties. Based on the exemptions in the proposed rule, OAG has minimized any potential adverse impact on small businesses while balancing the legislative intent of the Act.

The OAG will comply with section 202-b(6) of the State Administrative Procedure Act by publishing a summary of the proposed rule in the State Register and posting the proposed rule on OAG's website. In addition, OAG will conduct outreach with interested and potentially affected businesses, including trade organizations representing potentially covered operators.

Section 1508 of the Act specifies that only OAG may bring actions to enforce the Act. It further specifies that OAG may not bring any enforcement action until 180 days after the Act's effective date, which occurs 180 days after the promulgation of a final implementing rule by OAG. As the Act already provides for a 360-day period during which covered operators will have notice of their obligations and may prepare to comply with the rule without fear of enforcement actions, OAG preliminarily concludes that providing an additional cure period would go beyond the legislative intent.